Course Title:	Content Area:	Grade Level:	Credit (if applicable)
AP Cybersecurity	CTE	10-12	1.0

Course Description:

The AP Cybersecurity course provides a broad introduction to the field, aligning closely with a standard first-year collegiate introductory cybersecurity course. The course is designed to train students to:

- Understand Risk: Students learn about common threats and vulnerabilities and how they combine to create risk for individuals and organizations.
- Apply Defense-in-Depth: A central focus is studying how risk can be mitigated through a defense-in-depth strategy, which implements layered security controls.
- Secure Multiple Domains: Students explore specific vulnerabilities, attacks, mitigations, and detection measures across several key domains, including:
  - Physical spaces
  - Computer networks
  - Digital devices
  - Applications and data
- Evaluate Societal Impact: Throughout their studies, students consider the broader impact of cybersecurity on individuals, organizations, societies, and governments.

AP developed the course in partnership with college faculty and industry leaders, the course also aligns with the NICE Workforce Framework*. It emphasizes hands-on learning through authentic unit scenarios that connect classroom knowledge to real-world professional tasks.

**The NICE Workforce Framework for Cybersecurity, commonly referred to as the NICE Framework is developed by the National Institute for Standards and Technology (NIST) under the U.S. Department of Commerce. It is a nationally focused resource to help employers develop their cybersecurity workforce and it establishes a common lexicon that describes cybersecurity work and workers regardless of where or for whom the work is performed. The NICE Framework applies across public, private, and academic sectors. https://niccs.cisa.gov/tools/nice-framework*

Aligned Core Resources:	Connection to the ***BPS Vision of the Graduate***

• AP Cybersecurity Course and Exam Description
• AP Classroom: A dedicated online platform that provides a variety of resources and tools to offer yearlong support and meaningful feedback on student progress. These resources include:
  ○ Unit Guides
  ○ Lesson Plans
  ○ Professional Skills and Collaboration Rubrics
  ○ Practice Tests
  ○ Data Reports
  ○ Unit Scenarios
	Successfully Employ Skills for Self-Sufficiency
	• Goal Directed: As a "Career Kickstart" course, it prepares students for high-skill, high-growth careers by aligning with the NICE Workforce Framework. By earning an employer-endorsed credential, students demonstrate the ability to determine a career path that leads to self-sufficiency.
	Meaningfully Contribute to a Global Society
	• Collaboration: Collaboration is a core skill category (Category 4) in the AP framework. Students must work effectively with diverse teams to develop shared team objectives, determine clear roles, and assume responsibility for collaborative tasks.
	• Global Awareness: The course requires students to consider the impact of cybersecurity on societies and governments. This connects to the Vision of the Graduate's emphasis on understanding the global implications of decisions and staying informed about governmental processes and legal regulations like the Privacy Act of 1974.
	Effectively Communicate in a Global Society
	• Communication: Students must articulate thoughts effectively by explaining key cybersecurity concepts and communicating solutions to technical problems in both written and oral forms.
	• Information and Media Literacy: The course develops students' abilities to assess the credibility of sources, analyze digital messages, and identify phishing tactics. Students learn the ethical and legal issues surrounding the use of media and sensitive information.
	• Technology Literacy: Students use digital technology and networks (firewalls, VPNs, and Linux-based systems) to access, manage, and evaluate information, which is central to functioning in a modern knowledge society.

	Demonstrate Academic Knowledge and Skills • Content Mastery: Students develop a baseline understanding of academic disciplines within the Bristol curriculum by mastering introductory college-level cybersecurity content. • Critical Thinking and Problem Solving: The framework is an "unflinching encounter with evidence," requiring students to analyze risk, solve authentic problems through unit scenarios, and reflect critically on learning processes and solutions.
Additional Course Information: ***Knowledge/Skill Dependent courses/prerequisites***	**Link to *Completed Equity Audit***
There are no specific course prerequisites for AP Cybersecurity. The curriculum is designed with the following expectations regarding student readiness and course alignment: • Skill Requirements: Success in the course relies heavily on collaboration skills, which are considered critical to the deep understanding and application of cybersecurity knowledge. • Course Alignment: AP Cybersecurity is designed to be the equivalent of a one-semester introductory college course in cybersecurity. It is a part of the Career and Technical Education (CTE) Digital Technology cluster. • Foundational Knowledge: Unit 1 provides a starting point for all students, no prior technical security knowledge is required to begin the course.	AP Cybersecurity

Standard Matrix

Skill Standard	Unit 1	Unit 2	Unit 3	Unit 4	Unit 5
Skill 1: Analyze Risk - Evaluate risk to organizational assets.					
1.A Identify, with and without the support of AI, vulnerabilities, threats, and attack methods, and explain how they generate risk.	X				
1.B Determine ways adversaries exploit vulnerabilities to compromise an asset.	X				
1.C Evaluate, with and without the support of AI, the likelihood and impact of risks.			X	X	
1.D Document, with and without the support of AI, the likelihood and impact of risks.			X	X	
Skill 2: Mitigate Risk - Implement protective and deterrent security controls.					
2.A Identify security controls, and explain how they mitigate risks.	X	X	X	X	X
2.B Determine layered security controls that address vulnerabilities.		X		X	X
2.C Evaluate, with and without the support of AI, the impact of protective risk-management strategies.			X	X	
2.D Implement and log mitigations with and without the support of AI.			X	X	X
Skill 3: Detect Attacks - Implement detection methods, monitor systems, and analyze evidence.					
3.A Identify methods for monitoring systems, and explain how they detect attacks.	X	X			
3.B Determine strategies and methods to detect attacks.		X			X
3.C Evaluate the impact of threat detection methods.			X		
3.D Detect and classify cyberattacks by analyzing digital evidence with and without the support of AI.					X
Skill 4: Collaborate - Work with others and AI to accomplish a task.					
4.A Develop clear, shared team objectives related to a	X	X	X	X	X

cybersecurity task.					
4.B Determine clear roles and responsibilities for members of a team working to accomplish a cybersecurity task.	X	X	X	X	X
4.C Implement AI as a collaboration tool individually and as a group.	X	X	X	X	X
4.D Complete assigned work to accomplish a collaborative cybersecurity task.	X	X	X	X	X

Unit Links

Unit 1: Introduction to Security
Unit 2: Securing Spaces
Unit 3: Securing Networks
Unit 4: Securing Devices
Unit 5: Securing Applications and Data

Unit Title:

Unit 1: Introduction to Security

Relevant Standards:

Skill 1: Analyze Risk - Evaluate risk to organizational assets.

1.A Identify, with and without the support of AI, vulnerabilities, threats, and attack methods, and explain how they generate risk.

1.B Determine ways adversaries exploit vulnerabilities to compromise an asset.

Skill 2: Mitigate Risk - Implement protective and deterrent security controls.

2.A Identify security controls, and explain how they mitigate risks.

Skill 3: Detect Attacks - Implement detection methods, monitor systems, and analyze evidence.

3.A Identify methods for monitoring systems, and explain how they detect attacks.

Skill 4: Collaborate - Work with others and AI to accomplish a task.

4.A Develop clear, shared team objectives related to a cybersecurity task.

4.B Determine clear roles and responsibilities for members of a team working to accomplish a cybersecurity task.

4.C Implement AI as a collaboration tool individually and as a group.

4.D Complete assigned work to accomplish a collaborative cybersecurity task.

Essential Question(s):	**Enduring Understanding(s):**
• How do adversaries use social engineering to manipulate human behavior, and what are the potential impacts of these tactics? • In what ways do adversaries exploit weak authentication to compromise systems, and how can individuals strengthen their authentication to protect themselves? • What are the specific hazards associated with using public Wi-Fi networks, and what actions can individuals take to protect sensitive data while online? • How can adversaries leverage AI-powered tools to augment cyberattacks through impersonation or more convincing phishing? • How can cyber defenders use AI-powered tools to enable faster and more accurate threat detection and response? • How do the skill level and motivation of an adversary influence the nature of a cyberattack?	• Adversaries use social engineering and psychological tactics to manipulate human behavior, tricking individuals into revealing sensitive information or compromising their own security. • Systems are frequently compromised through weak authentication; however, individuals can significantly mitigate this risk by using multifactor authentication (MFA) and password managers to create long, unique, and random credentials. • Public Wi-Fi networks present unique hazards, such as evil twin and jamming attacks, where adversaries can capture network traffic or cause a denial of service (DoS). Protection requires verifying network authenticity and using virtual private networks (VPNs) to encrypt traffic. • Artificial Intelligence significantly augments the cybersecurity landscape. Adversaries use AI for voice cloning, digital avatars, and creating convincing phishing messages. Conversely, cyber defenders leverage AI to analyze millions of digital events at a scale impossible for humans, enabling faster and more accurate threat detection and response. • System vulnerabilities provide avenues for attack, and the resulting risk is a combination of the likelihood of an attack and the potential impact. • Cyberattacks can be identified by monitoring systems for indicators of compromise, such as unusual login times, failed authentication attempts, or suspicious network traffic logs.
Demonstration of Learning:	**Pacing for Unit**
Authentic unit scenarios designed to connect cybersecurity concepts to real-world personal security situations (see Lesson Sequence). Formal demonstration of learning is measured through multiple-choice questions on the AP Exam. Cumulative learning is measured through multiple-choice	5 Block Periods 1 Topic per Day • Topic 1.1: Understanding Social Engineering • Topic 1.2: Suspicious Website Logins • Topic 1.3: Best Practices for Public Networks • Topic 1.4: AI-Based Cybersecurity Attacks • Topic 1.5: Leveraging AI in Cyber Defense

questions on the AP Exam, which weigh Skill Category 1 (Analyze Risk), Skill Category 2 (Mitigate Risk), and Skill Category 3 (Detect Attacks) equally at 25–40% each across the entire course content.	
Family Overview (link below)	**Integration of Technology:**
AP Cybersecurity Family Overview	• Generative AI • Large Language Models (LLMs) • Multifactor Authentication (MFA) • Password Managers • Virtual Private Networks (VPNs) • Public Wi-Fi and Encryption • Wi-Fi router authorization logs
Unit-specific Vocabulary:	**Aligned Unit Materials, Resources, and Technology (beyond core resources):**
• Social engineering • Elicitation • Intimidation • Urgency • One-time password (OTP) • Multifactor authentication (MFA) • Password manager • Indicators of compromise (IoC) • Zero day • Evil twin attack • Jamming attack • Denial of service (DoS) • War driving • Virtual private network (VPN) • Generative AI / Large Language Models (LLMs) • Digital avatar • Shared secrets • Probabilistic calculations • Training sets	N/A
Opportunities for Interdisciplinary Connections:	**Anticipated misconceptions:**
• Human Behavior: Students explore how adversaries leverage common psychological principles to influence targets. • Emotional Manipulation: The curriculum covers the use of intimidation (leveraging a natural human aversion to negative consequences) and urgency (exploiting the impulse to react quickly to time-sensitive needs) to manipulate victims into bypassing their normal safety considerations. • Data Privacy Laws: Instruction is expected to integrate federal regulations such as the Privacy Act of 1974, the Children's Online Privacy Protection Act (COPPA), and the Health Insurance Portability and Accountability Act (HIPAA). • Professional Norms: The course connects to ethics by sharing norms from professional organizations like ISC2 and the UK Cyber Security Council. • Industry Regulation: Connections can be made to business and finance through the Payment Card Industry Data Security Standard (PCI DSS), which regulates the security of credit card data.	• Adversaries on a public Wi-Fi network can read all of a user's traffic. • Using a Virtual Private Network (VPN) makes a user's activity completely private from everyone. • Artificial Intelligence (AI) will replace the need for human cybersecurity professionals. • Phishing attempts are always easy to identify because of poor grammar or unnatural language. • If a system uses voice or image-based authentication, it is immune to remote impersonation. • AI tools like chatbots are safe places to enter any data for analysis. • Absolute security can be achieved if the right tools are used.

• Probability: AI-powered threat detection tools rely on probabilistic calculations to report the likelihood that a digital event is malicious. • Generative AI: Students study Large Language Models (LLMs) and how their training sets can be poisoned with false information, which connects to data science and linguistics. • Adversary Motivations: Students identify different types of adversaries whose motivations may be political, ideological, or belief-based. • Societal Impact: The unit encourages students to consider how cybersecurity affects societies and governments, particularly regarding the protection of sensitive public data and infrastructure.	
Connections to Prior Units:	**Connections to Future Units:**
N/A	• In Unit 2 (Securing Spaces), students are expected to practice selecting physical security controls based on the principles from Unit 1. • The core strategy of defense-in-depth, which focuses on layered security controls, is a recurring theme that students apply to networks in Unit 3, devices in Unit 4, and applications in Unit 5. • Risk Assessment: Unit 1 introduces identifying vulnerabilities and potential avenues of attack. This matures into formal risk assessment processes in Unit 2 (Topic 2.1) and is applied to complex network and device scenarios in Units 3 and 4. • Indicators of Compromise (IoCs): The concept of detecting attacks by analyzing log files for signs of suspicious activity (IoCs) begins in Unit 1 with unauthorized logins (Scenario 1B). This skill is built upon in Unit 3 for network attacks, Unit 4 for device password attacks, and Unit 5 for application-level attacks like SQL injection. • Authentication: The basic principles of strong authentication and multifactor authentication (MFA) from Topic 1.2 are expanded in Unit 4, where students learn the technical details of hashing and salt. • Artificial Intelligence (AI): The dual-use nature of AI for attack and defense introduced in Topics 1.4 and 1.5 is revisited in Unit 3, where students evaluate how AI-powered tools enable faster, more accurate detection on massive enterprise networks. • Encryption and VPNs: The individual use of VPNs and protocol sensitivity discussed in Unit 1 (Topic 1.3) sets the stage for the formal study of cryptography, symmetric vs. asymmetric encryption, and organizational VPN policies in Units 3 and 5.

Differentiation through *Universal Design for Learning*

	Engagement	Representation	Action & Expression
1.1A	"Can You Spot the Phish?" gamified challenge analyzing real and simulated email/SMS lures.	Color-coded infographic highlighting red flags (urgent tone, mismatched domain, generic greeting).	Create an annotated "Phishing Anatomy" breakdown poster or record a screencast walkthrough.
1.1B	Role-play exercise simulating social engineering tactics like urgency and authority.	Mind map illustrating psychological triggers (fear, scarcity, trust, authority).	Write a psychological case analysis or record a podcast episode on why victims comply.

1.1C	Real-world breach case studies exploring individual and corporate fallout.	Dual-column matrix categorizing impacts across financial, operational, and reputational scales.	Present a news broadcast report or draft an executive breach impact summary.
1.2A	Interactive password-cracking time estimator demonstrating brute-force speeds.	Flowchart comparing brute-force, dictionary, and credential stuffing attack mechanisms.	Design a password safety awareness flyer or construct an interactive quiz.
1.2B	"Crack the Default" challenge attempting login on default credentials in isolated VMs.	Step-by-step graphic showing entry points via weak, reused, or unhashed passwords.	Write an IT advisory memo or draw an explanatory technical comic strip.
1.2C	Hands-on experience setting up Multi-Factor Authentication (MFA) and password managers.	Layered graphic illustrating authentication factors (Something you know, have, are).	Draft a personal password policy guide or produce an MFA video tutorial.
1.3A	Threat actor card-sorting game matching motives, tools, and targets.	Continuum chart mapping threat actors from script kiddies to nation-states.	Create a threat actor dossier portfolio or record a mock intelligence briefing.
1.3B	Interactive simulation of Evil Twin access points and packet eavesdropping.	Network topology diagram showing Evil Twin, Jamming, and MitM attack vectors.	Design a public Wi-Fi security checklist or demonstrate wireless threat mitigations.
1.3C	Scenario-based "Remote Worker Challenge" securing public Wi-Fi connections.	Visual guide detailing VPN encryption, auto-connect settings, and HTTPS enforcement.	Produce an employee travel safety video or draft a remote work wireless policy.
1.4A	Audio and video analysis of AI voice cloning and deepfake phishing examples.	Comparative visual showing traditional phishing vs. AI-driven spear-phishing.	Write an analytical essay or record a video reflection on AI attack scaling.
1.4B	"Outsmart the AI" challenge enforcing out-of-band verification protocols.	Process map showing multi-channel identity verification and cryptographic checks.	Build an organizational verification decision tree or record a training video.
1.5A	Test automated static code analyzers and AI security review tools.	Workflow visual showing parallel manual and AI automated code analysis.	Write a comparative analysis report or present a live demonstration of AI code scanning.
1.5B	Anomaly detection game identifying statistical outliers in network traffic datasets.	Visual graph contrasting baseline user behavior with anomaly probability thresholds.	Construct a technical slide deck or present an interactive probability model.

Supporting Multilingual/English Learners (*CELP standards*)

	Emerging	Expanding	Bridging
1.1A	Select or circle visual examples/phishing red flags (e.g., suspicious sender, urgent language) from a given sample email using a bilingual word bank.	Highlight and label social engineering red flags in sample emails/texts, explaining in complete sentences using sentence starters (*"The indicator is ____ because ____"*).	Identify and categorize subtle indicators of social engineering in multi-stage attack scenarios, explaining reasoning in technical prose.
1.1B	Match social engineering psychological triggers (e.g., *urgency, fear, authority*) to visual scenarios using graphic organizers.	Explain the victim influence cycle using guided paragraph frames (*"Attackers use [trigger] to make victims feel [emotion], which leads them to [action]"*).	Draft a detailed analysis explaining how combined psychological triggers manipulate human behavior in corporate settings.
1.1C	Identify and sort impact icons (e.g., *financial loss, data theft, reputation damage*) into cause-and-effect visual charts.	Write short paragraph descriptions of attack consequences using transition words (*as a result, consequently, leads to*).	Compose a comprehensive impact assessment detailing short-term and long-term organizational and personal consequences.
1.2A	Match password attack descriptions (e.g., *brute force, credential stuffing*) to illustrative diagrams or log entry snippets using a glossary.	Identify signs of password attacks in log snippets using key vocabulary (*failed attempts, lockouts, rate limiting*).	Synthesize multiple system log entries to detect and distinguish between brute force, dictionary, and spray password attacks.
1.2B	Complete cloze (fill-in-the-blank) sentences describing weak password exploitation using word banks and diagrams.	Explain exploitation mechanisms using cause-and-effect sentence frames (*"Adversaries exploit [weakness] by [action], which results in [compromise]"*).	Formulate a technical explanation detailing how adversaries bypass single-factor or weak authentication systems.

1.2C	Label multi-factor authentication (MFA) components (e.g., *something you know, have, are*) on a visual diagram.	Explain how MFA and password managers increase security using comparative sentence frames (*"MFA is stronger than passwords alone because..."*).	Compare and justify complex authentication architecture enhancements (e.g., FIDO2/WebAuthn, biometric policies) in an executive summary.
1.3A	Classify adversary profiles into a T-chart (*Low-Skilled / Script Kiddie* vs. *High-Skilled / APT*) using provided trait cards.	Write comparative statements distinguishing adversary skill levels based on motivation, tools, and resources using graphic organizers.	Analyze complex threat intelligence briefs to identify, classify, and profile adversary skill levels and sophistication.
1.3B	Match terms (e.g., *evil twin, rogue AP, jamming*) to visual illustrations of wireless network topologies.	Describe wireless attack mechanisms using sequence frames (*"First, the attacker sets up... Next, the user connects..."*).	Evaluate wireless threat vectors in various physical environments and document specific attack signatures.
1.3C	Match protective actions (e.g., *use VPN, disable auto-connect*) to corresponding wireless threats using icon cards.	Describe recommended wireless security measures in written paragraphs using advisory language (*"Users should...", "Organizations must..."*).	Develop and justify a comprehensive wireless security protocol for remote and mobile workers.
1.4A	Identify examples of AI-augmented attacks (e.g., *voice cloning, automated phishing*) using side-by-side visual comparisons.	Explain how AI enhances attack speed and scale using graphic organizers and cause-and-effect prompts.	Analyze complex AI threat scenarios (e.g., deepfakes, AI-generated polymorphic code) and articulate adversary capabilities.
1.4B	Sequence visual steps for verifying AI-driven communications (e.g., *out-of-band verification, authentication phrase*).	Summarize countermeasures against AI-driven attacks using structured writing frames (*"To defend against AI voice cloning, organizations can..."*).	Critically evaluate defense mechanisms against advanced AI threat vectors and propose multi-layered mitigation strategies.
1.5A	Match AI defensive capabilities (e.g., *automated code auditing, anomaly detection*) to simple definitions using a visual glossary.	Explain defensive AI applications in structured paragraphs using targeted academic language (*analyze, detect, automate, audit*).	Write a detailed proposal outlining how AI tools can be integrated into continuous integration/continuous deployment (CI/CD) pipelines for security.
1.5B	Order a simplified flow chart showing data input $\rightarrow$ probabilistic calculation $\rightarrow$ threat alert.	Explain probabilistic threat scoring using guided prompts (*"AI calculates probability by comparing [baseline] to [anomaly]..."*).	Mathematically and conceptually explain how machine learning models utilize baseline behavior metrics to reduce time-to-detect (TTD).

Unit Outline

Lesson Sequence	Learning Target	Success Criteria	Assessment
DAY 1 1.1 Understanding Social Engineering	**1.1.A:** Identify common indicators of social engineering tactics.	Attacks use psychological tactics (elicitation) to manipulate users into revealing data or clicking malicious links/files. Tactics include intimidation (threats of negative consequences) and urgency (pressure to act quickly).	**Scenario 1A:** Detecting Phishing Messages Students can analyze a simulated email to identify psychological triggers like urgency and intimidation and describe the potential impact of clicking malicious links.
	1.1.B: Explain how social engineering tactics influence victims.	Tactics rely on psychological principles influencing human behavior. Intimidation uses fear and aversion to negative outcomes. Urgency prevents users from taking time to consider if an action is safe or reasonable.	
	1.1.C: Describe possible impacts of attacks.	Disclosure of personal info leading to impersonation or compromised challenge questions. Disclosure of one-time passwords (OTP) or login codes.	

		Installation of malware or capture of credentials via fake websites.	
DAY 2 1.2 Suspicious Website Logins	**1.2.A:** Identify common signs of a password attack.	Adversaries use common/stolen passwords and patterns to log in. Signs include many failed attempts, unusual login times, or unknown devices.	**Scenario 1B:** Detecting Unauthorized Logins. Students can analyze a Wi-Fi router authorization log to identify suspicious patterns, such as multiple failed attempts in a short duration or unknown devices.
	1.2.B: Explain how adversaries exploit weak authentication.	Users often use predictable patterns (names, dates, simple combinations). Adversaries use automated tools and gathered personal info to run dictionary attacks.	
	1.2.C: Explain how to make authentication stronger.	Use long, random, and unique passwords; employ password managers. Avoid personally meaningful words/numbers. Enable multifactor authentication (MFA) for an extra layer of proof.	
DAY 3 1.3 Best Practices for Public Networks	**1.3.A:** Identify the type of adversary (low- vs. high-skilled)	Adversaries range from low-skilled (using purchased tools) to high-skilled (creating tools and finding zero day vulnerabilities). Motivations include greed, recognition, politics, or specific causes.	**Scenario 1C:** Impacts of Using Public Wi-Fi Students can explain the hazards of fake captive portals and describe how to verify network authenticity before connecting to public Wi-Fi.
	1.3.B: Identify types of wireless attacks.	Evil twin attack: Setting up a malicious WAP with a similar name to a target network. Jamming attack: Flooding an area with EM signals to cause a denial of service (DoS). War driving: Detecting wireless beacons while moving around a target area.	
	1.3.C: Describe protection actions.	Consider data sensitivity (like DNS queries) before joining unencrypted networks. Verify that the network name matches the intended network exactly. Use a virtual private network (VPN) to encrypt traffic to the provider's system.	
DAY 4 1.4 AI-Based Cybersecurity Attacks	**1.4.A:** Explain how adversaries use AI to augment attacks.	Creating digital avatars (voice/image) for impersonation. Generative AI (LLMs) creating native-sounding phishing messages in any language. Prompt injection to extract sensitive info from LLMs. Poisoning training sets with false information. AI-powered reconnaissance of social media/public data. AI-enhanced coding for malware or finding software vulnerabilities.	**Scenario 1D:** AI-Powered Cyberattacks Students can describe how to verify an individual's identity during a suspected scam call by establishing and using shared secrets.
	1.4.B: Explain how to	Establish shared secrets (secret words) with	

	protect against AI attacks.	family/friends to verify identity. Use MFA to block access even if voice authentication is bypassed. Avoid entering sensitive data into AI chatbots. Verify AI output with reputable, non-AI-based sources.	
<u>DAY 5</u> 1.5 Leveraging AI in Cyber Defense	**1.5.A:** Explain how defenders use AI to protect data and review code. **1.5.B:** Explain how AI enables faster threat detection through probabilistic calculations.	Recommending secure configurations for firewalls and access controls. Analyzing application code for vulnerabilities. Suggesting detection rules for automated systems. Humans cannot examine the millions of daily digital network events. AI sorts malicious activity from harmless events at scale. AI can alert personnel or take programmed corrective actions automatically. Enables rapid intervention to prevent infrastructure damage and data loss.	**Scenario 1E:** AI-Powered Cyber Defense. Students can analyze the role of human oversight in AI-driven security, explaining why security technicians must review AI-generated code fixes or detector rules.

Unit Title:

Unit 2: Securing Spaces

Relevant Standards:

Skill 2: Mitigate Risk - Implement protective and deterrent security controls.

2.A Identify security controls, and explain how they mitigate risks.

2.B Determine layered security controls that address vulnerabilities.

Skill 3: Detect Attacks - Implement detection methods, monitor systems, and analyze evidence.

3.A Identify methods for monitoring systems, and explain how they detect attacks.

3.B Determine strategies and methods to detect attacks.

Skill 4: Collaborate - Work with others and AI to accomplish a task.

4.A Develop clear, shared team objectives related to a cybersecurity task.

4.B Determine clear roles and responsibilities for members of a team working to accomplish a cybersecurity task.

4.C Implement AI as a collaboration tool individually and as a group.

4.D Complete assigned work to accomplish a collaborative cybersecurity task.

Essential Question(s):	**Enduring Understanding(s):**
• Why is physical security considered a critical first layer of defense in a defense-in-depth cybersecurity strategy? • How do adversaries leverage a combination of social engineering and physical tactics to bypass security measures and gain unauthorized access? • In what ways can an organization evaluate, document, and prioritize the risks posed by various physical vulnerabilities? • What are the different strategies for managing physical risk (avoidance, transference, mitigation, and acceptance), and how do organizations determine which are most appropriate? • How do physical, technical, and managerial controls work together to create a resilient, layered defense for an organization's assets? • How can monitoring equipment and personnel be effectively placed and utilized to detect physical security breaches? • How do the different types of adversaries (e.g., script kiddies vs. hacktivists) and their motivations influence the physical threats an organization must defend against?	• Securing physical spaces is a critical first layer of defense in a comprehensive security strategy. If an adversary gains physical access to a device, they can often bypass technical controls that protect the system and its data. • A defense-in-depth (layered defense) strategy is essential because it provides resilience. By using multiple types of security controls (physical, technical, and managerial), an organization ensures that if one control is bypassed, another may still prevent or limit damage. • Absolute security is unattainable. Organizations must focus on risk management, which involves identifying and mitigating vulnerabilities while ultimately accepting a level of residual risk. • Risk is not a vague concept but a calculable combination of the likelihood of an attack and the severity of the potential damage. Once assessed, risks are managed through one of four primary strategies: avoidance, transference, mitigation, or acceptance. • Effective security requires adversarial thinking, which involves identifying vulnerabilities and attack methods to determine the best selection and placement of protective and detective controls. • Physical security is not just about locks and fences; it also involves protecting against social engineering tactics like piggybacking and tailgating, where adversaries manipulate authorized individuals to gain access.
Demonstration of Learning:	**Pacing for Unit**
Authentic unit scenarios designed to connect cybersecurity concepts to real-world personal security situations (see Lesson Sequence). Formal demonstration of learning is measured through multiple-choice questions on the AP Exam. Cumulative learning is measured through multiple-choice questions on the AP Exam, which weigh Skill Category 1 (Analyze Risk), Skill Category 2 (Mitigate Risk), and Skill Category 3 (Detect Attacks) equally at 25–40% each across the entire course content.	11 Block Periods • Topic 2.1: Cyber Foundations: ~ 4 Blocks • Topic 2.2: Physical Vulnerabilities and Attacks: ~ 3 Blocks • Topic 2.3: Protecting Physical Spaces: ~ 2 Blocks • Topic 2.4: Detecting Physical Attacks: ~ 2 Blocks
Family Overview (link below)	**Integration of Technology:**

AP Cybersecurity Family Overview	• Cameras and Visual Recording • Integrated Sensing • Biometric and Recognition Software • Entry Logs and Sensors • Hardware and Physical Access Controls • Access Control Systems • Port Security • Power Resilience • AI-Supported Analysis
Unit-specific Vocabulary:	**Aligned Unit Materials, Resources, and Technology (beyond core resources):**
• Pretexting • authority • intimidation • consensus • scarcity • familiarity • urgency • script kiddies • hacktivists • insider threats (insider adversaries) • cyberterrorists • transnational criminal organizations • reconnaissance • initial access • persistence • lateral movement • taking action • evading detection • open source intelligence (OSINT) • command and control (C2) protocol • remote access trojan (RAT) • rootkit • asset • likelihood • severity • vulnerability • avoidance • transference • mitigation • acceptance • residual risk • confidentiality • integrity • physical controls • technical controls • managerial controls • preventative controls • detective controls • corrective controls • defense-in-depth • piggybacking • tailgating • shoulder surfing • dumpster diving • card cloning • bollards • fencing	N/A

• access control vestibules • turnstiles • card readers • uninterruptible power supply (UPS) • power generators • security awareness training • workstation security policy • clean desk policy • motion sensors • stationary vs. patrolling security guards • facial recognition software • audit and evidence	
Opportunities for Interdisciplinary Connections:	**Anticipated misconceptions:**
• Psychology and Behavioral Science: The study of social engineering (Topic 2.1) is deeply rooted in psychology. Students analyze how adversaries use specific psychological tactics to manipulate human behavior. This connects to behavioral science concepts of how humans respond to pressure, fear, and social norms. • Sociology and Political Science: The classification of adversaries (Topic 2.1) connects to sociology and political science by examining the motivations behind attacks. Students study hacktivists motivated by social or political causes and cyberterrorists who seek to disrupt civil infrastructure, such as power grids, to impact entire regions or nations. This encourages an understanding of how external social and political beliefs can manifest as technical threats. • Cost-Benefit Analysis: Students must determine "cost-effective" solutions, where the price of a security control is weighed against the expected financial loss from an attack. • Risk Management Strategies: Concepts like risk transference (e.g., using insurance) and risk acceptance are standard business operations used to handle organizational uncertainty. • Impact Assessment: Students evaluate the severity of damage not just in technical terms, but also through financial, operational, and reputational costs. • Architecture: Students engage in workplace-style tasks like reviewing building plans to identify vulnerabilities and strategically placing physical barriers such as bollards, fencing, and access control vestibules. • Physical Engineering: Students study the engineering of power resilience through Uninterruptible Power Supplies (UPS) and generators. • Law and Ethics: The course requires the integration of legal and professional norms throughout all units. In Unit 2, this connects to Civics and Law as students learn about regulations like the Privacy Act of 1974, HIPAA, and industry-specific rules like PCI DSS. They	• Over-Reliance on Technical Controls • The Pursuit of "Absolute Security" • Limiting Social Engineering to the Digital Realm • "More is Better" in Detection Technology • Conflating Security Control Functions • Motivation vs. Skill of Adversaries

also consider the broader impact of cybersecurity on societies and governments.	
Connections to Prior Units:	**Connections to Future Units:**
• Application of Risk Management Principles: Students in Unit 2 practice selecting security controls based on the principles introduced in Unit 1. While Unit 1 focuses on identifying vulnerabilities and mitigating risks at a personal level, Unit 2 applies these skills to physical organizational assets, such as securing a research lab. • Continuity of Social Engineering Tactics: Unit 1 and 2 place heavy emphasis on the human element of security. Unit 1 introduces how adversaries use psychological triggers like urgency and intimidation to influence behavior through digital means like phishing. Unit 2 expands this by showing that social engineering is also a primary tool for conducting physical attacks. Students learn how tactics like familiarity and consensus are used in person to facilitate breaches like piggybacking. • Evolution of Detection and Log Analysis: The skill of detecting attacks through indicators of compromise (IoCs) is a major thread. In Unit 1, students learn to identify signs of suspicious activity—such as many failed login attempts—by analyzing digital log files. In Unit 2, this skill is applied to physical entry logs. Students analyze how long electronic doors remain open to detect patterns that signify tailgating or unauthorized access. • Adversary Classification: Unit 2 provides more granular detail on the types of adversaries first mentioned in Unit 1. Unit 1 establishes the baseline classification of adversaries by skill level (low-skilled vs. high-skilled). Unit 2 builds on this by identifying specific groups, such as script kiddies, hacktivists, and insider threats, and exploring their unique motivations and methods. • Ongoing Role of Artificial Intelligence (AI): The course-wide theme of leveraging AI-powered tools continues. Just as students in Unit 1 see how defenders use AI for code review and threat detection, students in Unit 2 are expected to use AI to support risk assessment and identify physical vulnerabilities.	Building the Defense-in-Depth Strategy: Unit 2 introduces the concept of defense-in-depth (layered defense), where students learn that physical security is necessary because gaining physical access often allows an adversary to bypass many technical controls. Future units add subsequent layers to this model: • Unit 3 adds the network layer (firewalls, segmentation). • Unit 4 adds the device layer (antimalware, host-based firewalls). • Unit 5 adds the application and data layer (encryption, access controls). Evolution of Risk Assessment: The formal risk assessment process taught in Topic 2.1 is the exact framework students apply to different domains in every future unit: • In Unit 3, students assess risk from network vulnerabilities. • In Unit 4, they evaluate risks from device-specific vulnerabilities. • In Unit 5, they analyze risks to sensitive applications and files. Progression of Log Analysis and Detection: Unit 2 establishes the skill of detecting attacks by analyzing logs (specifically physical entry logs). This skill matures through the following units: • Unit 3: Students analyze network traffic logs and packet captures to find indicators of compromise (IoCs) like ARP poisoning or smurf attacks. • Unit 4: Students review authentication logs for signs of password attacks like spraying or credential stuffing. • Unit 5: Students examine web application and server logs for injection-type attacks like SQLi or directory traversals. Physical Access vs. Technical Port Security: Unit 2 introduces the vulnerability of exposed device ports in physical spaces. This connects directly to future technical mitigations: • Unit 3 explores port security on switches to prevent adversaries from plugging in rogue access points. • Unit 4 teaches students how to configure BIOS/UEFI protection to prevent adversaries from booting into unauthorized modes if they have physical access to a device. Protection of Data at Rest: Unit 2 emphasizes protecting the physical environment where data is stored (e.g., locking server rooms). Unit 5 connects this to the states of data, specifically data at rest, noting that it is critical to protect the physical drive from theft or destruction before even applying digital encryption.

Differentiation through *Universal Design for Learning*

	Engagement	Representation	Action & Expression
2.1A	Physical security escape-room puzzle focusing on tailgating and baiting.	Visual matrix categorizing tailgating, impersonation, and dumpster diving.	Build a physical security assessment rubric or design front-desk safety training slides.
2.1B	Case study analysis comparing malicious insiders vs. external physical intruders.	Venn diagram illustrating motives, access levels, and capabilities of physical adversaries.	Produce a physical threat actor infographic or write an insider threat risk profile.

2.1C	Cyber Kill Chain mapping activity tracking a breach from recon to exfiltration.	Sequential visual timeline mapping the 7 Cyber Kill Chain stages.	Construct a breach timeline storyboard or present a historic cyberattack case study.
2.1D	Facility inspection activity evaluating vulnerabilities in a physical classroom/lab.	Flowchart illustrating Risk = Asset x Threat x Vulnerability.	Draft a facility Risk Assessment Report or create an interactive risk evaluation matrix.
2.1E	"Risk Budgeting" simulation deciding to Accept, Avoid, Mitigate, or Transfer risks.	2x2 Risk Decision Matrix (Impact vs. Likelihood) mapped to management strategies.	Present a business pitch justifying risk management choices or write a policy proposal.
2.1F	Hands-on sorting game classifying Physical, Technical, and Managerial controls.	Multi-tier grid categorizing controls by type and function (Deterrent, Preventative, Detective).	Create a security control index poster or code a review quiz application.
2.1G	"Swiss Cheese Model" physical demonstration showing layered defense overlap.	Concentric circle diagram showing physical, network, host, and data defenses.	Build a 3D/digital model of layered defenses or present a Defense-in-Depth plan.
2.2A	Virtual walk-through audit of server rooms spotting physical security flaws.	Taxonomy chart detailing physical attack vectors (lock picking, rogue drop boxes).	Conduct a physical facility audit report supported by photos or video clips.
2.2B	Scenario simulation analyzing cascading failures from physical disruptions.	Cause-and-effect (Fishbone) diagram linking physical gaps to asset destruction.	Write a physical vulnerability failure report or record a brief security briefing.
2.2C	Physical penetration tester role-play evaluating facility access points.	Standardized physical security assessment checklist with risk rating scales.	Deliver a formal Physical Security Audit Document with weighted risk scores.
2.3A	Review corporate visitor logs and badge policy documents.	Visual policy hierarchy detailing visitor escorting, badging, and clean-desk policies.	Draft a Physical Security Standard Operating Procedure (SOP) manual.
2.3B	"Facility Redesign" challenge modifying physical layouts to enhance security.	Before-and-after floorplan blueprints incorporating mantraps, bollards, and locks.	Present an architectural security proposal or design an interactive floorplan.
2.4A	Hands-on inspection of motion detectors, glass-break sensors, and CCTV analytics.	Hardware diagram mapping infrared, acoustic, and magnetic sensors to zones.	Record a video demonstration or write a technical buyer's guide for detection hardware.
2.4B	"Blind Spot Elimination" game placing virtual sensors for optimal coverage.	Heatmap visual overlay on floorplans showing sensor ranges and blind spots.	Present a sensor placement architectural diagram supported by technical justifications.
2.4C	Investigate physical security logs and badge reader timestamp discrepancies.	Event timeline correlating badge access logs with physical CCTV footage.	Write an incident forensic report or present a timeline analysis slide deck.

Supporting Multilingual/English Learners (*CELP standards*)

	Emerging	Expanding	Bridging
2.1A	Categorize scenario flashcards into attack types (e.g., *phishing, vishing, tailgating, shoulder surfing*).	Write brief scenario descriptions identifying social engineering attack types with supporting clues.	Analyze complex physical and digital social engineering scenarios to identify underlying attack vectors.
2.1B	Match threat actor names (e.g., *insider, nation-state, hacktivist*) to primary motive keywords and images.	Describe adversary motivations and capabilities using comparative graphic organizers.	Profile threat actors in real-world case studies and detail their tactical tendencies and resource levels.
2.1C	Sequence visual cards representing the Cyber Kill Chain / attack lifecycle (e.g., *Recon, Access, Execution*).	Describe each phase of a cyberattack using sequential transition words (*initially, subsequently, ultimately*).	Map complex multi-stage real-world attacks across standard frameworks (e.g., MITRE ATT&CK, Cyber Kill Chain).
2.1D	Complete a visual Risk Matrix (Asset, Threat, Vulnerability) using color-coded cards (High, Medium, Low).	Explain the risk assessment steps using paragraph frames and formulas.	Conduct a quantitative and qualitative risk assessment for a given scenario and articulate findings in a formal report.
2.1E	Sort risk responses into four bins: *Accept, Avoid, Mitigate, Transfer* using scenario prompts.	Explain choices for risk management strategies using conditional frames ("*If the risk is too costly, the organization should transfer it by...*").	Justify optimal risk management decisions based on cost-benefit analysis and business continuity requirements.

2.1F	Classify controls into categories (*Technical, Operational, Physical*) using a picture-supported sorting mat.	Describe the functions of control categories (*Preventative, Detective, Corrective*) using targeted technical vocabulary.	Evaluate existing security controls within an enterprise architecture and identify missing control types.
2.1G	Label the layers of the "Swiss Cheese" or defense-in-depth model on a graphic diagram.	Explain defense-in-depth using analogy frames ("*Defense-in-depth is like a castle because...*").	Formulate a technical defense-in-depth architecture plan defending against single points of failure across an organization.
2.2A	Label physical threat illustrations (e.g., *tailgating, dumpster diving, badge cloning, lock picking*).	Write short descriptions of physical security breaches observed in provided case study diagrams.	Distinguish between subtle physical attack techniques and document physical breach indicators.
2.2B	Match physical vulnerabilities (e.g., *unlocked doors, unshredded paper*) to potential asset damage/loss.	Explain cause-and-effect relationships between physical vulnerabilities and business disruption using structured prompts.	Synthesize physical threat scenarios to project potential operational, financial, and physical impacts on assets.
2.2C	Complete a fill-in checklist rating physical vulnerabilities observed in a site floor plan image.	Draft structured risk assessment notes using a provided vulnerability-impact table template.	Conduct a comprehensive physical security audit and produce a standardized risk documentation matrix.
2.3A	Match physical security managerial terms (e.g., *visitor logs, clean desk policy, security training*) to pictures.	Explain the purpose of physical security policies using modal verbs ("*Employees must lock...*", "*Visitors should...*").	Draft clear, enforceable managerial control policies for physical access control and asset protection.
2.3B	Select appropriate physical mitigations (e.g., *mantrap, bollards, CCTV, badges*) from a visual choice board for given threats.	Explain selected physical mitigation strategies using justification sentence frames ("*We chose [control] in order to prevent [threat]*").	Develop a comprehensive physical security mitigation proposal tailored to high-risk facilities.
2.4A	Circle physical detection devices in a facility diagram (e.g., *motion sensors, CCTV, door contact sensors*).	Describe how specific physical security controls alert security personnel using sequential language.	Analyze physical detection control capabilities and evaluate their responsiveness to diverse attack vectors.
2.4B	Place physical security control icons on a building floor plan map at appropriate entry/exit points.	Justify placement of detection controls on a facility floor plan using spatial prepositions (*adjacent to, perimeter, bottleneck*).	Design an optimized physical sensor placement layout that minimizes blind spots and maximizes coverage.
2.4C	Match security sensor alert logs (e.g., "*Door 3 forced open*") to corresponding physical incidents.	Interpret physical security alert logs and describe the likely incident using structured reporting templates.	Correlate physical access control logs and video surveillance data to reconstruct physical security incidents.

Unit Outline

Lesson Sequence	Learning Target	Success Criteria	Assessment
DAY 1 -2 2.1 Part 1 Cyber Foundations	**2.1.A:** Identify social engineering attacks.	Adversaries use psychological tactics such as pretexting, authority, intimidation, consensus, scarcity, familiarity, and urgency to manipulate targets into a desired action.	**Defense in Depth**: Professional Skills/Collaboration Rubrics. Students can accurately classify adversaries (e.g., script kiddies vs. hacktivists) and explain psychological tactics like pretexting or consensus in a formative quiz. **Lesson Plans provided by AP Classroom.** Students create a visual model of a layered defense for an organization, documenting how physical, technical, and
	2.1.B: Identify types of adversaries.	Adversaries include script kiddies, hacktivists, insider threats, cyberterrorists, and transnational criminal organizations, each with distinct motivations ranging from greed to political beliefs.	
DAY 3 -4 2.1 Part 2 Cyber Foundations	**2.1.C:** Describe the phases of a cyberattack.	The typical phases are reconnaissance, initial access, persistence, lateral movement, taking action, and evading detection.	
	2.1.D: Describe the risk assessment process.	Risk assessment evaluates the likelihood and severity of an attack against a specific vulnerability for an	

		asset.	managerial controls work together.
	2.1.E: Identify strategies for managing risk.	Organizations manage risk through avoidance, transference, mitigation, and acceptance.	
	2.1.F: Identify types of security controls.	Controls address confidentiality, integrity, or availability (CIA) and are classified by type (physical, technical, managerial) and function (preventative, detective, corrective).	
	2.1.G: Explain why a defense-in-depth security strategy is necessary to optimally protect an organization.	Defense-in-depth (layered defense) provides resilience so that if one control is bypassed, another may still prevent or limit damage.	
DAY 5 -7 2.2 Physical Vulnerabilities and Attacks	**2.2.A:** Identify common physical attacks.	Common attacks include piggybacking, tailgating, shoulder surfing, dumpster diving, and card cloning.	**Scenario 2A (Xtensr Labs)**: Building and physical plans; AI-powered tools for risk documentation. **Scenario 2A Part 1:** Students review building plans for Xtensr Labs to identify vulnerabilities and document the likelihood and severity of potential attacks.
	2.2.B: Explain how threats can exploit common physical vulnerabilities to cause loss, damage, disruption, or destruction to assets.	Physical access can allow adversaries to disrupt power, steal information, or install malware via open device ports.	
	2.2.C: Assess and document risks from physical vulnerabilities.	Risks range from high (unrestricted access to sensitive systems) to low (unsecured low-value assets).	
DAY 8 -9 2.3 Protecting Physical Spaces	**2.3.A:** Identify managerial controls related to physical security.	Controls include security awareness training and a workstation security policy (e.g., clean desk policies, privacy screens).	**CED Topic 2.3**; Examples of Workstation Security and Clean Desk policies. **Scenario 2A Part 2:** Students recommend specific mitigations (e.g., bollards, access control vestibules) and draft a Workstation Security Policy.
	2.3.B: Determine mitigation strategies for risks from physical vulnerabilities.	Mitigations include physical barriers (fencing, bollards), locks, card readers, access control vestibules, and uninterruptible power supplies (UPS).	
DAY 10-11 2.4 Detecting Physical Attacks	**2.4.A:** Identify ways security controls can detect physical attacks.	Detection methods include cameras, security guards, motion sensors, and alert employees.	**Entry Logs**: Motion sensor and camera placement diagrams; AI for threat detection. Students analyze entry logs to detect "indicators of compromise" like tailgating and propose camera/sensor placement to minimize false alarms.
	2.4.B: Determine effective placement of security controls for detecting physical attacks.	Controls should be placed at points of ingress/egress and areas where traffic is unexpected, like server rooms.	
	2.4.C: Apply detection techniques to identify physical attacks.	Techniques include using facial recognition, pairing motion detectors with cameras, and reviewing entry logs for signs of piggybacking or tailgating.	

Unit Title:

Unit 3: Securing Networks

Relevant Standards:

Skill 1: Analyze Risk - Evaluate risk to organizational assets.

1.C Evaluate, with and without the support of AI, the likelihood and impact of risks.

1.D Document, with and without the support of AI, the likelihood and impact of risks.

Skill 2: Mitigate Risk - Implement protective and deterrent security controls.

2.A Identify security controls, and explain how they mitigate risks.

2.C Evaluate, with and without the support of AI, the impact of protective risk-management strategies.

2.D Implement and log mitigations with and without the support of AI.

Skill 3: Detect Attacks - Implement detection methods, monitor systems, and analyze evidence.

3.C Evaluate the impact of threat detection methods.

Skill 4: Collaborate - Work with others and AI to accomplish a task.

4.A Develop clear, shared team objectives related to a cybersecurity task.

4.B Determine clear roles and responsibilities for members of a team working to accomplish a cybersecurity task.

4.C Implement AI as a collaboration tool individually and as a group.

4.D Complete assigned work to accomplish a collaborative cybersecurity task.

Essential Question(s):	**Enduring Understanding(s):**
• How does the transmission of data between devices create new opportunities for adversaries, and how can defenders protect data while it is in transit? • What are common network-based attacks (such as ARP poisoning, DNS poisoning, and Smurf attacks), and how do they exploit specific network vulnerabilities? • Why is network segmentation (using subnets, VLANs, and DMZs) a critical strategy for isolating traffic and preventing an adversary's lateral movement? • How do firewalls use Access Control Lists (ACLs) to manage the flow of traffic, and why is their strategic placement and rule precedence vital for network security? • In what ways do automated security tools, such as NIDS, NIPS, and SIEM, allow organizations to monitor systems and detect malicious activity more effectively? • How can organizations leverage Artificial Intelligence (AI) and probabilistic models to manage massive amounts of network data and enable faster threat detection? • What are the trade-offs between different detection methods (signature-based, anomaly-based, and hybrid) regarding speed, cost, and human factors like alert fatigue?	• The transmission of data between devices through a computer network creates significant opportunities for adversaries. • Dividing a network into smaller, isolated segments (subnets or VLANs) is a critical defensive strategy. It isolates network traffic, which can prevent a security breach on one subnet from impacting devices on other subnets and limits an adversary's ability to move laterally across the network. • Effective network security requires the strategic deployment of multiple technical controls, including firewalls to manage traffic flow and wireless encryption (such as WPA3) to ensure data confidentiality. • Firewalls use Access Control Lists (ACLs) to permit or deny traffic based on specific criteria like IP addresses and ports. Because these rules are executed in a specific precedence order, the sequence in which they are written directly determines the network's security posture. • While humans cannot analyze the millions of digital events occurring daily, automated tools and Artificial Intelligence (AI) can quickly sort and classify data patterns to identify malicious activity. • Organizations must choose between signature-based (efficient for known threats) and anomaly-based (better for novel attacks) detection. These choices involve balancing factors such as false positive rates, which can lead to alert fatigue, and false negative rates, which allow adversaries to bypass detection.
Demonstration of Learning:	**Pacing for Unit**
Authentic unit scenarios designed to connect cybersecurity concepts to real-world personal security situations (see Lesson Sequence). Formal demonstration of learning is measured through multiple-choice questions on the AP Exam. Cumulative learning is measured through multiple-choice questions on the AP Exam, which weigh Skill Category 1 (Analyze Risk), Skill Category 2	14 Block Periods • Topic 3.1: Network Vulnerabilities and Attacks: ~ 3 Blocks • Topic 3.2: Protecting Networks: Managerial Controls and Wireless Security: ~ 2 Blocks • Topic 3.3: Protecting Networks: Segmentation: ~ 1 Block • Topic 3.4: Protecting Networks: Firewalls: ~ 4 Blocks • Topic 3.5: Detecting Network Attacks: ~ 4 Blocks

(Mitigate Risk), and Skill Category 3 (Detect Attacks) equally at 25–40% each across the entire course content.	
Family Overview (link below)	**Integration of Technology:**
AP Cybersecurity Family Overview	• Firewall Configuration • Segmentation Tools • Secure Architectures • Automated Monitoring and Detection Systems • Network Intrusion Detection Systems (NIDS) and Network Intrusion Prevention Systems (NIPS) • Log Aggregation (SIEM): Security Information and Event Management • Vulnerability Scanning • Virtual Private Networks (VPNs).
Unit-specific Vocabulary:	**Aligned Unit Materials, Resources, and Technology (beyond core resources):**
• On-path Attack (Man-in-the-Middle) • ARP Poisoning • MAC Spoofing • MAC Flooding • DNS Poisoning • Smurf Attack • Distributed Denial of Service (DDoS) • Jamming Attack • Network Segmentation • Subnetting • VLAN (Virtual Local Area Network) • Screened Subnet (DMZ) • Port Security • Access Control List (ACL) • Rule Precedence • Stateless Firewall • Stateful Firewall (Dynamic Packet Filtering) • Next-Generation Firewall (NGFW) • VPN (Virtual Private Network) • WPA3 • Beacon Frame • NIDS / NIPS • SIEM (Security Information and Event Management) • Signature-Based Detection • Anomaly-Based Detection • False Positive / False Negative • Alert Fatigue • Probabilistic Calculations	N/A
Opportunities for Interdisciplinary Connections:	**Anticipated misconceptions:**
• Healthcare Law: Scenario 3A (Protecting Patient Medical Data) requires students to secure internal file servers containing patient records. This connects to the Health Insurance Portability and Accountability Act (HIPAA), which regulates the protection of health information (PHI). • Military and National Security: Scenario 3C places students in the role of a technician on a naval submarine, managing secure networks for weapons systems and operations. This provides a	• The "More is Better" Fallacy in Detection • Order Irrelevance in Firewall Rules • Conflating Detection (NIDS) with Prevention (NIPS) • Overestimating AI's Certainty • Misunderstanding the Limits of Signature-Based Detection • Confusing Network Segmentation with Physical Separation

window into the ethics and protocols of national defense and military-grade cybersecurity. • Probability and Statistics: Students study how Artificial Intelligence (AI) algorithms use probabilistic calculations to report a percentage likelihood that a specific activity pattern is malicious. • Quantitative Analysis: Students must evaluate the trade-offs of detection methods based on statistical rates of false positives and false negatives, which determine the effectiveness of a system and the risk of alert fatigue. • Electromagnetics: Students learn to detect jamming attacks by scanning for electromagnetic (EM) noise within the wireless frequency range. • Geometry and Signal Analysis: The curriculum mentions using signal triangulation to locate and disable unauthorized wireless access points (evil twins). • Financial Regulations: Protecting networks that handle transactions connects to the Payment Card Industry Data Security Standard (PCI DSS). • Resource Management: Students evaluate the impact of SIEM systems that aggregate logs from multiple sources to detect broad patterns, mirroring business intelligence and operational oversight tasks. • Economic Evaluation: The unit requires students to evaluate security controls based on cost versus speed of detection, ensuring that the chosen tools fit within an organization's budget. • Public Service and Emergency Management: Scenario 3B connects cybersecurity to disaster relief. Students must set up a secure wireless network at an emergency shelter following a natural disaster to provide internet access for displaced families. This demonstrates how cybersecurity is a foundational component of modern civil service and crisis management.	
Connections to Prior Units:	**Connections to Future Units:**
• Progression of the Defense-in-Depth Model: Unit 3 adds a critical layer to the defense-in-depth (layered defense) strategy introduced in Unit 2. While Unit 2 focuses on the physical perimeter (locks, cameras, guards) as the first layer of defense, Unit 3 transitions to the network layer, teaching students how to protect devices once they are connected and communicating. • Application of the Risk Assessment Framework: The formal risk assessment process defined in Unit 2 is the exact framework students apply to networking in Unit 3. In this unit, students move from assessing physical risks (like an unlocked door) to technical network risks (like an improperly configured firewall). • Evolution of Log Analysis and Detection: The practice of identifying indicators of compromise	Progression of the Defense-in-Depth Strategy: Unit 3 focuses on the network layer of defense. This connects directly to: • Unit 4 (Device Layer): Students learn that while Unit 3 firewalls protect the network perimeter, devices require their own security because adversaries who bypass network controls (or operate from within the network) must be stopped at the host level. • Unit 5 (Application/Data Layer): This represents the final and most critical layer. Unit 3 teaches how to protect data in transit across the network, while Unit 5 focuses on protecting that same data at rest and in use. Evolution of Firewall Logic: The technical logic of filtering traffic introduced in Unit 3 is directly applied in Unit 4: • In Unit 3, students master network-based firewalls, using Access Control Lists (ACLs) and rule precedence to manage traffic flow between network segments. • In Unit 4, students apply these exact same principles—ACLs, rule order, and permitting/denying by IP and port—to configure host-based firewalls that protect individual devices.

(IoCs) through log analysis is a continuous thread throughout the course:
    - Unit 1: Students analyze digital logs for unauthorized website logins.
    - Unit 2: Students analyze physical entry logs to detect tailgating or piggybacking.
    - Unit 3: Students refine these skills by analyzing network log files and packet captures to identify technical attacks like ARP poisoning or Smurf attacks.
- Adversary Tactics and Phases: The types of adversaries (e.g., script kiddies, hacktivists) and the phases of a cyberattack (reconnaissance, initial access, lateral movement, etc.) introduced in Unit 2 provide the context for the network attacks studied in Unit 3. Unit 3 specifically explores how adversaries use network vulnerabilities to facilitate lateral movement, a concept first defined as a key phase of an attack in Unit 2.
- VPNs: Unit 1 introduces Virtual Private Networks (VPNs) as a personal tool to protect sensitive data on public Wi-Fi. Unit 3 expands this concept into a professional managerial control, where students learn to develop organizational VPN policies for secure remote access.
- Artificial Intelligence: The theme of leveraging AI in cyber defense started in Unit 1. Unit 3 provides a more technical explanation of how AI algorithms use probabilistic calculations to sort through the millions of digital events logged on networks daily, a task impossible for human teams alone.

Scaling Detection and Log Analysis: The skill of identifying Indicators of Compromise (IoCs) through digital evidence matures across the units:
- Unit 3 focuses on network-based IoCs found in traffic patterns, such as ARP poisoning or Smurf attacks.
- Unit 4 shifts to host-based IoCs, where students analyze authentication logs for signs of credential stuffing or password spraying.
- Unit 5 culminates in application-based IoCs, such as detecting SQL injection or XSS signatures within web application and server logs.

From Network Encryption to Data Cryptography: Unit 3 introduces encryption as a tool for securing communication channels, which is expanded in Unit 5:
- Unit 3 focuses on protocol-specific encryption, such as WPA3 for wireless networks and VPNs for remote access.
- Unit 5 dives into the mathematical foundations of cryptography (symmetric vs. asymmetric algorithms), teaching students the underlying mechanics that make the network-level encryption they used in Unit 3 possible.

Mitigating Lateral Movement: A central theme of Unit 3 is network segmentation (using VLANs, subnets, and DMZs) to prevent an adversary's lateral movement.
- This connects to Unit 4 and Unit 5, which explore the consequences of failed segmentation. In these units, students see how an adversary who successfully moves laterally can exploit device vulnerabilities (Unit 4) to ultimately reach their end goal: stealing or destroying sensitive data (Unit 5).

Consistent Application of Risk Assessment: The risk assessment framework (identifying assets, vulnerabilities, threats, likelihood, and impact) practiced in Unit 3 is the standard methodology students will use for the remainder of the course.
- In Unit 4, they apply it to IoT and smart devices.
- In Unit 5, they apply it to proprietary data and web applications.

Differentiation through *Universal Design for Learning*

	Engagement	Representation	Action & Expression
3.1A	Packet inspection activity identifying MitM, DDoS, and ARP spoofing patterns.	Visual diagrams illustrating packet manipulation during network attacks.	Create a network attack cheat sheet or record a packet capture (Pcap) analysis.
3.1B	Lab simulation of unencrypted HTTP traffic sniffing using Wireshark.	Side-by-side packet flow diagrams comparing plaintext vs. TLS encrypted traffic.	Write a network exploit report or give a technical walk-through of packet interception.
3.1C	Network scanning challenge using Nmap in a sandbox to discover open ports.	Risk matrix mapping open ports and unpatched services to exploit severity.	Compile an Nmap vulnerability scan report with documented risk scores.
3.2A	Debate session on network Acceptable Use Policies (AUP) and access rules.	Organizational hierarchy chart linking network governance to policy enforcement.	Draft an Acceptable Use Policy (AUP) document or record a policy video.
3.2B	Sandbox lab configuring router settings (WPA3, SSID hiding, MAC filtering).	Step-by-step visual screenshot guide for wireless router security hardening.	Produce a router security tutorial video or submit a lab configuration portfolio.
3.3A	Design a network topology for a company balancing guest, employee, and server traffic.	Network architecture diagram showing VLANs, subnets, and micro-segmentation.	Build a topology in Cisco Packet Tracer or construct a physical network diagram.
3.3B	Simulation comparing blast radius of malware on flat vs. segmented networks.	Comparative animation showing lateral movement restrictions within VLANs.	Write an executive memo advocating network segmentation or deliver a presentation.

3.4A	Feature-matching game comparing packet-filtering, stateful, and Next-Gen Firewalls.	Feature table mapping OSI layers (Layer 3/4 vs. Layer 7) to firewall types.	Create a firewall decision guide infographic or record an explanatory mini-lecture.
3.4B	"Firewall Bouncer" activity filtering incoming packets based on ACL rule sets.	Color-coded ACL table displaying Source/Destination IP, Port, Protocol, Action.	Write an ACL rule set for a business scenario or record a rule evaluation video.
3.4C	Virtual lab placing firewalls in DMZ and internal positions to block traffic.	Network architectural diagram highlighting DMZ positioning and firewall placement.	Submit a firewall configuration file or present a firewall placement diagram.
3.5A	Inspection of Intrusion Detection (IDS) vs. Intrusion Prevention Systems (IPS) alerts.	Workflow chart contrasting passive monitoring (IDS) vs. active blocking (IPS).	Create an IDS/IPS comparison chart or produce an explanatory video.
3.5B	Case study on AI SIEM tools detecting automated network anomalies.	Infographic tracing AI SIEM data ingestion, event correlation, and automated isolation.	Write a research summary or present a proposal on AI threat detection adoption.
3.5C	Scenario challenge selecting between signature, heuristic, or behavioral detection.	Decision tree graphic guiding selection of detection methods based on threat types.	Draft a network defense strategy paper justifying selected detection methods.
3.5D	Analysis of false positives vs. false negatives and impact on SOC team fatigue.	Trade-off spectrum chart balancing detection sensitivity with network performance.	Draft a detection impact evaluation report or present a cost-benefit analysis.
3.5E	"Log Forensics Detective" activity analyzing firewall/server logs for indicators of compromise.	Highlighted log file cheat sheet with key fields (Timestamp, Source IP, Event Code).	Write an incident forensic report or present a web log analysis walkthrough.

Supporting Multilingual/English Learners (*CELP standards*)

	Emerging	Expanding	Bridging
3.1A	Match network attack names (e.g., *DoS/DDoS, Man-in-the-Middle, Spoofing*) to simple network diagrams.	Write definitions of network attacks using provided technical vocabulary and key phrase starters.	Categorize and contrast advanced network attack vectors based on OSI model layers and execution mechanisms.
3.1B	Fill in diagram callouts showing how an attacker intercepts or floods unencrypted network traffic.	Explain network vulnerability exploitation using step-by-step cause-and-effect frames.	Analyze network topology diagrams to identify exploited protocol weaknesses (e.g., unencrypted HTTP, ARP poisoning).
3.1C	Complete a guided risk matrix for network assets (e.g., *unpatched router, open ports*).	Write network risk statements using the format: "*The network is vulnerable to [threat] because of [vulnerability], leading to [impact]*".	Formulate comprehensive network risk assessment documentation including likelihood, impact, and risk scores.
3.2A	Match network security policies (e.g., *Acceptable Use Policy, Password Policy*) to illustrative rule cards.	Describe the objective of network security managerial controls using imperative and regulatory language.	Author operational network security policies that align with industry frameworks (e.g., NIST SP 800-53).
3.2B	Follow a step-by-step visual screenshot guide to select *WPA3* encryption and change default SSIDs on a router GUI.	Complete wireless security configuration tasks and explain chosen settings (*WPA3, disabled WPS*) using short notes.	Independently configure enterprise-grade wireless security parameters and document security posture choices.
3.3A	Color-code different network zones (e.g., *DMZ, Internal, Guest, IoT*) on a network architecture diagram.	Describe network segmentation techniques (e.g., *VLANs, Subnetting, Firewalls*) using descriptive paragraphs.	Design network segmentation schemes using subnets, VLANs, and micro-segmentation principles.
3.3B	Select visual choices demonstrating how a firewall/VLAN blocks lateral movement during a breach.	Explain how segmentation stops lateral movement using contrast frames ("*Without segmentation... However, with segmentation...*").	Evaluate network architecture designs and justify segmentation strategies to prevent breach propagation.
3.4A	Match firewall types (e.g., *Stateless, Stateful, Next-Gen/NGFW*) to feature summaries using graphic cards.	Describe differences between stateless, stateful, and application-level firewalls using comparative tables.	Analyze enterprise requirements to select and justify the deployment of specific firewall types.

3.4B	Circle *ALLOW* or *DENY* actions on sample firewall ACL rules based on source/destination IP matching prompts.	Explain how ACL rule order (*top-down processing*) affects firewall traffic filtering using conditional statements (*"If traffic matches rule 1..."*).	Write, critique, and optimize sequential firewall ACL rules to enforce least privilege access.
3.4C	Place firewall icons between network zones on a diagram and match pre-written rule blocks to interfaces.	Justify firewall placement at network boundaries and complete rule configuration exercises using guided templates.	Architect firewall network placement (e.g., dual-homed DMZ) and configure complex filtering rulesets.
3.5A	Label automated tools (e.g., *IDS, IPS, SIEM, Packet Sniffer*) on a network monitoring graphic.	Describe the function of automated network detection tools using targeted verbs (*monitors, alerts, blocks, logs*).	Compare passive detection (IDS) vs. active prevention (IPS) tools in enterprise network monitoring.
3.5B	Match AI detection features (e.g., *anomaly detection, automated threat isolation*) to visual scenario pairs.	Write short explanations describing how AI processes large log volumes to identify abnormal network traffic patterns.	Analyze the integration of AI-driven Threat Intelligence and SOAR (Security Orchestration, Automation, and Response) platforms.
3.5C	Select the appropriate detection method (e.g., *signature-based vs. anomaly-based*) using a simple decision flowchart.	Recommend signature-based or anomaly-based detection for specific scenarios using conditional sentence starters.	Justify the selection and integration of hybrid detection methodologies for complex network environments.
3.5D	Categorize detection results into a 2×2 grid (*True Positive, False Positive, True Negative, False Negative*).	Explain the operational impacts of *False Positives* vs. *False Negatives* on security teams using structured sentence frames.	Evaluate IDS/IPS performance metrics (precision, recall, alert fatigue) and recommend tuning adjustments.
3.5E	Highlight malicious indicators (e.g., *unusual port, repeated failed handshakes*) in simplified, highlighted network log samples.	Analyze Wireshark packet summaries or Syslog entries to identify attack signatures and document findings in writing frames.	Perform deep packet analysis and log evaluation to reconstruct network attack timelines and scope.

Unit Outline

Lesson Sequence	Learning Target	Success Criteria	Assessment
DAYS 1-3 3.1 Network Vulnerabilities & Attacks	**3.1.A:** Identify common network attacks.	Attacks include ARP poisoning (MAC spoofing), MAC flooding (eavesdropping/sniffing), DNS poisoning (credential harvesting), and Smurf attacks (DoS/DDoS).	**Scenario 3A:** Protecting Patient Medical Data. Students can identify and explain technical attacks such as ARP poisoning, DNS poisoning, and Smurf attacks. Students assess risk for Scenario 3A by identifying vulnerabilities in existing architecture.
	3.1.B: Explain exploitation of network vulnerabilities.	Vulnerabilities include improperly configured firewalls, open data ports, rogue access points, and unauthenticated networks.	
	3.1.C: Assess and document network risks.	Defenders use automated vulnerability scanners to evaluate risk levels (low, moderate, high) based on technical difficulty and potential impact on confidentiality, integrity, or availability.	
DAY 4-5 3.2 Managerial Controls & Wireless Security	**3.2.A:** Identify managerial controls for network security.	Managerial controls involve establishing organizational standards for router security, switch security, VPN usage, and wireless security policies.	**Scenario 3B:** Configuring a Secure Wireless Network. Students describe security configurations for Scenario 3B, including disabling beacon frames, managing signal strength, and implementing WPA3 encryption.
	3.2.B: Configure wireless network security features.	Technical mitigations include disabling beacon frames, controlling signal strength, using WPA3 encryption, and enabling MAC filtering.	
DAY 6 3.3 Best	**3.3.A:** Identify techniques for segmenting a network.	Techniques include creating a screened subnet (DMZ), subnetting via IP addressing, and utilizing VLANs on switches.	**Scenario 3C:** Protecting a Network on a Naval Submarine.

Practices for Public Networks	**3.3.B:** Explain why segmentation increases security.	Segmentation isolates traffic to prevent lateral movement, allows for diverse security policies across zones, and enables port security to prevent MAC flooding.	Students use a diagram to recommend security features for different LANs in Scenario 3C, demonstrating knowledge of VLANs, subnets, and screened subnets (DMZ).
DAY 7-10 3.4 Firewalls	**3.4.A:** Identify types of network firewalls.	Types include stateless (header-based filtering), stateful (dynamic packet filtering), and next-generation firewalls (NGFW) which offer deep packet inspection and application-type filtering.	**Scenario 3A Artifacts:** Students determine placement and configure Firewalls A and B for Scenario 3A. They must demonstrate proper ACL rule precedence to allow specific traffic (e.g., SSH, HTTP) while blocking malicious requests.
	3.4.B: Explain how firewalls use Access Control Lists (ACLs).	An Access Control List (ACL) permits or denies traffic based on direction, IP address, port, or service, with rules executed in a specific precedence order.	
	3.4.C: Determine placement and configure firewalls.	Firewalls should be placed at every point of ingress/egress between internal segments and the public internet. Configuration involves defining specific rules (e.g., Allow Inbound TCP port 22) to meet organizational security requirements.	
DAY 11-14 3.5 Detecting Network Attacks	**3.5.A:** Identify types of automated security tools used to detect network attacks.	Tools include NIDS (detection/alerting), NIPS (prevention/blocking), and SIEM systems (log aggregation and pattern analysis).	**Scenario 3B Detection Task:** Students analyze packet captures and logs to identify indicators of compromise (IoCs). They evaluate the impact of signature-based vs. anomaly-based detection, considering factors like false positives and alert fatigue.
	3.5.B: Explain how organizations can leverage artificial intelligence (AI) to enhance threat detection and response.	AI algorithms use probabilistic calculations to classify massive amounts of data as malicious or normal, helping to prevent alert fatigue.	
	3.5.C: Determine a network detection method.	Methods include signature-based (known patterns), anomaly-based (deviations from a baseline), or hybrid detection.	
	3.5.D: Evaluate the impact of a network detection method.	Impacts are evaluated based on speed, cost, and the rates of false positives (causing alert fatigue) versus false negatives (adversaries bypassing detection).	
	3.5.E: Apply detection techniques to identify indicators of network attacks by analyzing log files.	Techniques include signal triangulation for evil twins, scanning for EM noise for jamming, and monitoring for duplicate MAC addresses or ICMP spikes to find ARP poisoning or Smurf attacks.	

Unit Title:

Unit 4: Securing Devices

Relevant Standards: Bold indicates priority

Skill 1: Analyze Risk - Evaluate risk to organizational assets.

1.C Evaluate, with and without the support of AI, the likelihood and impact of risks.

1.D Document, with and without the support of AI, the likelihood and impact of risks.

Skill 2: Mitigate Risk - Implement protective and deterrent security controls.

2.A Identify security controls, and explain how they mitigate risks.

2.B Determine layered security controls that address vulnerabilities.

2.C Evaluate, with and without the support of AI, the impact of protective risk-management strategies.

2.D Implement and log mitigations with and without the support of AI.

Skill 4: Collaborate - Work with others and AI to accomplish a task.

4.A Develop clear, shared team objectives related to a cybersecurity task.

4.B Determine clear roles and responsibilities for members of a team working to accomplish a cybersecurity task.

4.C Implement AI as a collaboration tool individually and as a group.

4.D Complete assigned work to accomplish a collaborative cybersecurity task.

Essential Question(s):	**Enduring Understanding(s):**
• How do the diverse types of computing devices expand the attack surface and create unique vulnerabilities for adversaries to exploit? • In what ways do different types of malware, such as ransomware, rootkits, or fileless malware, enable adversaries to damage, disrupt, or gain unauthorized control of a device? • Why is cryptographic hashing fundamental to secure password storage, and how does the use of "salts" protect against attacks like rainbow tables? • How do various authentication factors (knowledge, possession, biometric, and location) and multifactor authentication (MFA) effectively verify user identity and prevent impersonation? • What is the role of managerial controls (such as Acceptable Use Policies) and host-based technical controls (like firewalls and anti-malware) in a defense-in-depth strategy? • How can security professionals identify and distinguish between host-based, file-based, and behavior-based indicators of compromise (IoCs) when analyzing device logs? • What are the trade-offs involved in selecting detection methods, specifically regarding the impact on device performance, cost, and the rate of false positives?	• Computing devices are the primary targets for adversaries because they store, process, and transmit all digital data. • The rapid integration of embedded computers into everyday items has led to a rapid growth in device vulnerabilities, requiring defenders to assess risk across a much broader range of hardware than traditional computers. • Securing individual devices is a critical layer in a defense-in-depth strategy; it provides a final opportunity to stop an adversary who has already bypassed physical and network-layer controls. • Cryptographic hash functions are fundamental to security because they produce a fixed-length output that is repeatable and one-way, allowing for the secure storage of passwords and the verification of data integrity without storing plaintext information. • Robust security requires verifying user identity through various factors (knowledge, possession, biometric, and location); implementing Multifactor Authentication (MFA) is significantly more secure than single-factor methods because it requires at least two separate proofs of identity. • Keeping a device's operating system and applications updated with patches is one of the most effective ways to prevent adversaries from taking advantage of known vulnerabilities. • Defenders can identify that a device has been compromised by analyzing Indicators of Compromise (IoCs) found in system logs, such as unusual file modifications, unexpected processes, or failed login patterns in authentication logs. • Organizations must evaluate detection methods based on cost, impact on device performance, and the trade-off between false positive rates (which cause alert fatigue) and the ease with which an adversary can bypass the system.
Demonstration of Learning:	**Pacing for Unit**

Authentic unit scenarios designed to connect cybersecurity concepts to real-world personal security situations (see Lesson Sequence). Formal demonstration of learning is measured through the AP Exam • Multiple Choice: Weighs Skill Category 1 (Analyze Risk), Skill Category 2 (Mitigate Risk), and Skill Category 3 (Detect Attacks) equally at 25–40% each across the entire course content. • Free-Response Question (FRQ): Unit 4 is a primary focus of the "Device Security Analysis" FRQ. In this section, students must analyze simulated sources to identify security issues and describe how specific configuration changes would impact the device and its users.	16 Block Periods • Topic 4.1: Device Vulnerabilities and Attacks: ~ 6 Blocks • Topic 4.2: Authentication: ~ 3 Blocks • Topic 4.3: Protecting Devices: ~ 3 Blocks • Topic 4.4: Detecting Attacks on Devices: ~ 4 Blocks
Family Overview (link below)	**Integration of Technology:**
AP Cybersecurity Family Overview	• Internet of Things (IoT) and Embedded Systems • Mobile and Server Infrastructure • Hashing Algorithms • Multifactor Authentication (MFA) • Endpoint Defense and Configuration Tools • Host-Based Firewalls • Anti-Malware Systems • Automated Patching • Connected Farm Equipment • Authentication Hardening • Manufacturing Forensics
Unit-specific Vocabulary:	**Aligned Unit Materials, Resources, and Technology (beyond core resources):**
• Servers • Personal Computers • Handheld Computers • Embedded Computers • Internet of Things (IoT) • BIOS / UEFI: Basic Input Output System or Unified Extensible Firmware Interface • Malware • Virus • Worm • Trojan • RAT (Remote Access Trojan) • Ransomware • Spyware • Keylogger • Logic Bomb • Rootkit • Fileless Malware • Cryptographic Hash Function • Collision • Plaintext • Salt • Multifactor Authentication (MFA) • Password Spraying • Credential Stuffing	N/A

• Rainbow Table Attack • Managerial Controls • Patch • Host-Based Firewall • Anti-Malware • Indicator of Compromise (IoC) • Authentication Logs (Auth Logs) • Host-Based IoC • File-Based IoC • Behavior-Based IoC • EDR (Endpoint Detection and Response)	
Opportunities for Interdisciplinary Connections:	**Anticipated misconceptions:**
• Precision Agriculture: Students research how internet-connected machinery, such as automated irrigation systems and milking machines, relies on onboard computers and GPS for remote maneuvering and operation. • Food Security: Analyzing vulnerabilities in farming equipment connects to larger issues of national food supply stability and the impact of cyberattacks on critical agricultural infrastructure. • Medical Equipment Security: Students examine the vulnerabilities of embedded computers within life-critical devices, such as pacemakers, insulin pumps, IV pumps, and MRI scanners. • Biometrics: The study of authentication factors includes biometric factors such as iris or retina scans and facial recognition, connecting cybersecurity to biological traits and physiology. • Cryptographic Hashing: Students study the properties of cryptographic hash functions (like SHA-256), exploring mathematical algorithms that take binary data of arbitrary length and produce a fixed-length string. • Probability and Logic: Learning about collisions (when two different inputs produce the same hash) and the keyspace of encryption algorithms involves statistical reasoning and binary logic. • Organizational Policy: Students analyze and develop managerial controls, such as Acceptable Use Policies (AUP), Password Policies, and Software Installation Policies, which govern professional behavior and legal compliance. • Risk Assessment: The unit mirrors professional business auditing by requiring students to document risks based on likelihood and severity, often measured by financial, reputational, or operational impact. • Infrastructure Management: Students learn about the specialized computers that operate critical infrastructure, such as circuit breakers at electrical substations and pumps at water treatment plants. • Industrial Forensics: Scenario 4C places students in the role of a forensic analyst for a manufacturing company, where they must protect industrial control environments from lateral movement following a breach.	• Internet of Things (IoT) as "Non-Computing" Devices • Confusing Hashing with Encryption • The Scope of Account Lockout Policies • Misunderstanding Multi-Factor Authentication (MFA) Factors. The "Best" Detection Method Fallacy • All Malware Is Contained in Files • Overestimating the Security of Mandatory Password Changes • Technical Application Errors (Permissions and Logs) • Misinterpreting Permission Bits • Conflating Authentication with Filtering
Connections to Prior Units:	**Connections to Future Units:**

- Integration into the Defense-in-Depth Model: Unit 4 represents a critical layer in the defense-in-depth (layered defense) strategy introduced in Unit 2. While Unit 2 focuses on the physical perimeter and Unit 3 on the network layer, Unit 4 focuses on the device layer. This unit teaches students that securing individual devices provides a final opportunity to stop an adversary who has already bypassed physical and network-layer controls.
- Application of the Risk Assessment Framework:The formal risk assessment process defined in Unit 2 is the exact framework students apply to devices in Unit 4. Students move from assessing physical risks (like an unlocked door) to technical device risks (like an unpatched operating system or an open telnet port).
- Evolution of Authentication and Identity Verification: Unit 4 builds upon the foundational security principles introduced in Unit 1:
    - Weak Authentication: While Unit 1 introduces the concept of weak passwords and unauthorized logins from a personal perspective, Unit 4 explores the technical mechanics of cryptographic hashing, salting, and rainbow table attacks.
    - Multifactor Authentication (MFA): Unit 1 introduces MFA as a personal tool. Unit 4 expands this into a technical requirement for organizational security, categorizing the specific factors used (knowledge, possession, biometric, and location).
- Progression of Log Analysis and Detection: The skill of identifying indicators of compromise (IoCs) through digital evidence is a continuous thread throughout the course:
    - Unit 1: Students analyze digital logs for unauthorized website logins.
    - Unit 3: Students analyze network log files and packet captures for network-based attacks.
    - Unit 4: Students refine these skills by analyzing authentication logs (auth logs) to identify host-based threats, such as password spraying or credential stuffing.
- Technical Logic of Firewalls: Unit 4 introduces host-based firewalls, which apply the same technical logic as the network-based firewalls studied in Unit 3. Students use the same principles of Access Control Lists (ACLs) and rule precedence (where the first matching rule is executed) to permit or deny traffic for a single device based on IP, port, and protocol.
- Managerial and Technical Controls: The classification of security controls (preventative, detective, and corrective) and control types (physical, technical, and managerial) from Unit 2 remains the standard for Unit 4.
    - Managerial Controls: Students expand on the policy work from Units 2 and 3 by developing device-specific policies, such as Acceptable Use
- Progression to the Final Defense-in-Depth Layer: Unit 4 represents the device layer of the defense-in-depth model. This connects directly to Unit 5, which addresses the final and most critical layers: applications and data. Students learn that while a device may be hardened (Unit 4), the ultimate goal of an adversary is often to steal, modify, or deny access to the data stored on that device (Unit 5).
- Evolution of Cryptographic Concepts
    - From Hashing to Encryption: In Unit 4, students master cryptographic hashing primarily for secure password storage and integrity checks.
    - Advanced Cryptography in Unit 5: Unit 5 builds on this by introducing symmetric and asymmetric encryption. Students apply their understanding of one-way hashes from Unit 4 to more complex two-way encryption processes used to protect data at rest and in transit.
- Scaling Access Control and Authorization
    - Unit 4 Hardening: Students learn to technically harden a device through login settings, such as password complexity and account lockout policies.
    - Unit 5 Access Models: Unit 5 expands these basic login configurations into formal Access Control Models, including Role-Based (RBAC), Discretionary (DAC), and Mandatory Access Control (MAC). The Linux-based permission skills (chmod, ls -l) introduced in Unit 4 assessments are core requirements for Scenario 5A.
- Maturation of Log Analysis and Detection: The practice of identifying Indicators of Compromise (IoCs) becomes more sophisticated in the transition to Unit 5:
    - Unit 4 focuses on host-based and behavior-based IoCs found in auth.log, such as password spraying or credential stuffing.
    - Unit 5 shifts to application-based IoCs. Students use the analysis skills they practiced in Unit 4 to identify more complex application-level attacks in web server logs, such as SQL injection, Cross-Site Scripting (XSS), and directory traversal.
- Progression of Managerial Controls:The policy-writing skills developed in Unit 4 are applied to more specialized data-handling contexts in Unit 5:
    - Unit 4 Policies: Focused on device behavior (Acceptable Use Policy) and local access (Password Policy).
    - Unit 5 Policies: Focused on specialized data protection, including Cryptography Policies and Web Application Security Policies.
- Realizing the Consequences of Lateral Movement: Unit 4 Scenario 4C requires students to analyze logs specifically to prevent a breach from spreading from a business network to a manufacturing network (lateral movement). This connects to Unit 5, where students see that the ultimate destination of lateral movement is typically to reach high-value, sensitive data (such as proprietary R&D) that must be protected with the application-level controls studied in the final unit.

Policies (AUP), Password Policies, and Software Installation Policies.
    - Technical Controls: Unit 4 focuses on host-level mitigations like anti-malware software and automated patching, which serve as the final technical barriers for a device.
- Continuous Use of AI as a Collaboration Tool: Building on Skill 4.C introduced in Unit 1, Unit 4 continues to integrate Artificial Intelligence as a collaborative partner. Students use AI to help research device vulnerabilities and analyze complex system logs, continuing the theme from Unit 3 where AI is used to sort through millions of data points to identify malicious patterns.

Differentiation through *Universal Design for Learning*

	Engagement	Representation	Action & Expression
4.1A	Endpoint sorting activity categorizing servers, IoT, embedded, and mobile devices.	Visual hardware/OS matrix mapping computing devices to attack surfaces.	Build an enterprise asset inventory list or create an interactive endpoint taxonomy graphic.
4.1B	"Malware Zoo" interactive exploration examining ransomware, trojans, worms, and spyware.	Taxonomy tree mapping malware categories to infection channels and payloads.	Design a malware identification poster or produce a podcast episode on malware defense.
4.1C	Demonstration of unpatched software exploits in isolated virtual machines.	Execution flow diagram showing buffer overflows and memory exploitation.	Write an endpoint exploit summary or record a screencast explaining exploitation.
4.1D	Perform an OS security audit on a sample image using CIS Benchmarks.	Scorecard rubric grading OS configurations, open services, and patch levels.	Produce an Endpoint Risk Assessment Report or present audit findings via video.
4.2A	Hands-on lab generating SHA-256 hashes to observe the avalanche effect.	Flowchart visual: Plaintext + Salt -> Cryptographic Hash Function -> Stored Hash.	Write an explanatory guide on hashing vs. encryption or record a hashing tool demo.
4.2B	Demonstration of offline hash cracking using weak vs. strong wordlists in a sandbox.	Conceptual diagram illustrating rainbow table attacks and unsalted hash risks.	Deliver a presentation on hash protection or write a whitepaper on salting.
4.2C	Scenario evaluation selecting Kerberos, OAuth, Biometrics, or RADIUS.	Comparison matrix evaluating authentication methods across security and usability.	Write an authentication architecture proposal or design a decision-tree graphic.
4.2D	Hands-on OS lab configuring lockout thresholds, complexity rules, and timeouts.	Screenshot walkthrough of Windows Group Policy or Linux PAM settings.	Submit a security policy configuration file or create an OS hardening lab guide.
4.3A	Policy evaluation review analyzing BYOD and Mobile Device Management (MDM) rules.	Policy chart contrasting BYOD, COPE, and CYOD management models.	Draft an MDM/BYOD corporate policy document or record an employee onboarding video.
4.3B	Demonstration comparing signature scanning vs. behavioral EDR blocking malware.	Dual-stream diagram showing malware execution interception and quarantine actions.	Write an endpoint security software recommendation memo or record a video explanation.
4.3C	Historical breach case study on unpatched system exploits (e.g., WannaCry).	Lifecycle diagram: Vulnerability Discovery -> Patch Release -> Testing -> Deployment.	Create a patch management policy guide or record a public service announcement video.
4.3D	Sandbox lab configuring Windows Defender Firewall or Linux ufw port rules.	Visual configuration guide mapping host firewall rules to specific ports.	Submit a host firewall hardening script or present a configuration walkthrough.
4.4A	Threat-hunting exercise identifying abnormal process tree executions.	Visual process tree diagram highlighting normal vs. malicious execution chains.	Write an endpoint threat-hunting guide or present a live process analysis demonstration.
4.4B	Selection evaluation choosing between Sysmon, OS audit logging, and EDR agents.	Selection matrix mapping telemetry requirements to specific logging tools.	Draft an endpoint detection strategy or build a tool selection presentation.

4.4C	Simulation measuring endpoint resource overhead (CPU/RAM) vs. logging verbosity.	Line graph balancing host performance impact against security visibility.	Write a performance-versus-security trade-off evaluation report.
4.4D	Analyze Event Logs (Event ID 4625) or Linux /var/log/auth.log for intrusion signs.	Event Log Cheat Sheet highlighting critical Event IDs and log parameters.	Create an event log forensic report or deliver a log analysis presentation.

Supporting Multilingual/English Learners (*CELP standards*)

	Emerging	Expanding	Bridging
4.1A	Label images of computing devices (e.g., *servers, endpoints, mobile devices, IoT, embedded systems*).	Classify computing devices by function and risk level using categorized graphic organizers.	Analyze diverse computing device hardware and firmware architectures for organizational security implications.
4.1B	Match malware types (e.g., *ransomware, spyware, Trojan, worm, rootkit*) to visual cartoons/icons and simple definitions.	Describe malware characteristics using classification matrices and guided summary frames.	Differentiate advanced malware behavior (e.g., fileless malware, polymorphic viruses) and propagation vectors.
4.1C	Trace an attack path diagram showing an unpatched system vulnerability leading to device compromise.	Explain how attackers exploit unpatched software or OS flaws using cause-and-effect sentence frames.	Analyze zero-day vs. known vulnerability exploitation techniques on endpoint operating systems.
4.1D	Complete a guided device inventory risk checklist using visual vulnerability indicators.	Document endpoint security risks using structured template fields (*Asset, Threat, Severity, Risk Level*).	Conduct comprehensive endpoint risk evaluations and generate formal risk documentation reports.
4.2A	Sequence a visual diagram: *Plaintext Password $\rightarrow$ Hash Function $\rightarrow$ Fixed Length Hash Digest*.	Explain password hashing and one-way functions using guided technical paragraph frames (*"Hashing transforms passwords into..."*).	Explain the mathematical and cryptographic properties of hashing algorithms (e.g., SHA-256) and collision resistance.
4.2B	Match attack methods (e.g., *rainbow tables, dictionary attacks, pass-the-hash*) to basic visual descriptions.	Explain how attackers crack hashes using rainbow tables or brute force through explanatory writing frames.	Contrast password cracking techniques and evaluate the effectiveness of cryptographic salts and key stretching (e.g., bcrypt).
4.2C	Sort authentication factors into three columns: *Something You Know, Something You Have, Something You Are*.	Classify multi-factor authentication methods and explain why multi-factor is superior to single-factor using comparative language.	Evaluate enterprise authentication frameworks (e.g., SAML, OAuth, PKI) for various device management scenarios.
4.2D	Follow step-by-step visual screenshots to configure password length, lockout thresholds, and screen timeouts in OS settings.	Configure endpoint security policies (e.g., Windows Group Policy / Linux PAM) and document configuration steps.	Script and enforce system-wide secure authentication and account lockout policies across enterprise devices.
4.3A	Match managerial device controls (e.g., *MDM policies, BYOD policy, asset tracking*) to workplace scenario cards.	Describe device management policies using policy language (*"Employees are required to...", "Unauthorized devices are..."*).	Formulate comprehensive Mobile Device Management (MDM) and Acceptable Use Policies (AUP) for enterprise endpoints.
4.3B	Complete fill-in sentences with a word bank explaining how anti-malware scans and isolates bad files.	Explain how anti-malware protects systems using technical verbs (*scans, quarantines, detects, updates signatures*).	Evaluate signature-based vs. heuristic/behavioral anti-malware solutions and their operational trade-offs.
4.3C	Sequence a diagram showing *Vulnerability Discovered $\rightarrow$ Patch Released $\rightarrow$ Patch Installed $\rightarrow$ System Secured*.	Write a short persuasive paragraph explaining why regular patching prevents malware exploitation using key vocabulary.	Formulate enterprise patch management lifecycle strategies, prioritizing critical security updates.
4.3D	Identify common endpoint attack symptoms (e.g., *high CPU usage, unexpected pop-ups, modified system files*) on an infographic.	Describe endpoint indicators of compromise (IoCs) in structured paragraphs using technical terminology.	Synthesize endpoint telemetry (process trees, memory dumps, registry changes) to detect host breaches.
4.4A	Match endpoint detection controls (e.g., *EDR, File Integrity Monitoring, Host IDS*) to corresponding threat descriptions.	Recommend endpoint detection controls for specific threat scenarios using justification sentence starters.	Architect an integrated endpoint detection strategy incorporating EDR, FIM, and centralized logging.

4.4B	Sort event scenarios into *High Impact / Immediate Alert* vs. *Low Impact / Log Only* visual bins.	Evaluate the effectiveness and system overhead impact of various host detection mechanisms using guided templates.	Perform trade-off analysis between detection sensitivity, resource consumption, and business operational disruption.
4.4C	Highlight suspicious log entries (e.g., *failed root login attempts, unauthorized PowerShell commands*) in annotated OS log files.	Analyze system log files (e.g., Windows Event Viewer, /var/log/auth.log) using guided search prompts and record IoCs.	Query and analyze raw host logs using SIEM search tools to construct incident response timelines.
4.4D	Label images of computing devices (e.g., *servers, endpoints, mobile devices, IoT, embedded systems*).	Classify computing devices by function and risk level using categorized graphic organizers.	Analyze diverse computing device hardware and firmware architectures for organizational security implications.

Unit Outline

Lesson Sequence	Learning Target	Success Criteria	Assessment
DAY 1-6 4.1 Device Vulnerabilities & Attacks	**4.1.A:** Identify types of computing devices.	Devices include servers, personal computers (laptops/desktops), handhelds (smartphones/tablets), embedded computers (specialized machines), and Internet of Things (IoT) devices (smart appliances, medical equipment, infrastructure pumps).	**Scenario 4A: Secure Connected Farm Equipment**; AI-supported risk evaluation tools. **Scenario 4A Part 1:** Students research how an adversary might exploit internet-connected farm equipment (IoT) and assess the risk level (likelihood and impact) for specific vulnerabilities.
	4.1.B: Identify types of malware.	Malware types include viruses (user-activated), worms (self-spreading), trojans (disguised as harmless), ransomware (file encryption), spyware, keyloggers, logic bombs, rootkits (operating system-level control), and fileless malware (RAM-based).	
	4.1.C: Explain exploitation of device vulnerabilities.	Vulnerabilities include unpatched software, weak authentication, lack of BIOS/UEFI protection (which allows booting into "recovery mode"), enabled autorun on external drives, open ports, and a lack of host-based firewalls or anti-malware.	
	4.1.D: Assess/document device risks.	Risks are classified as high (compromising sensitive data or critical operations like unpatched email servers), moderate (weak authentication for management systems), or low (low-impact vulnerabilities like an open telnet port on a standard laptop).	
DAY 7-9 4.2 Authentication Foundations	**4.2.A:** Explain password hashing.	The cryptographic hash function produces a fixed-length string that is collision-resistant, repeatable, and one-way (cannot be reversed). Hashing prevents plaintext password storage, while salting (adding random bits) ensures unique hashes for identical passwords.	**Scenario 4B: Aceshack Settings**; Password managers. **Scenario 4B:** Students log on as administrators to configure local security settings, such as password complexity, minimum length, and account-lockout policies to prevent brute-force attacks
	4.2.B: Explain password attack exploitation.	Attacks include online (active portal attempts), offline (running automated hash-cracking against stolen databases), password spraying (one password vs. many users), credential stuffing (using leaked/default credentials), and rainbow table attacks (precomputed hash lists).	
	4.2.C: Determine authentication types.	Authentication factors include knowledge (passwords/PINs),	

		possession (access cards/tokens), biometric (fingerprints/facial recognition), and location (GPS/IP address). Multifactor authentication (MFA) requires at least two separate factors.	
	4.2.D: Configure secure login settings.	Secure configurations include password complexity, minimum length, maximum age (periodic resets), password history (preventing reuse), and account lockout policies.	
DAY 10-12 4.3 Mitigating Device Risk	**4.3.A:** Identify managerial device controls.	Managerial controls include Acceptable Use Policies (AUP), Password Policies, and Software Installation Policies that define permitted activities and required security standards for organizational devices.	**Scenario 4A Part 2:** Students determine mitigation strategies for farm equipment, recommending host-based firewalls, anti-malware, and Acceptable Use Policies (AUP) to produce a report for management.
	4.3.B: Explain anti-malware software benefits.	Anti-malware uses signatures (indicators) to scan, quarantine, and remove malicious files that match its database.	
	4.3.C: Explain the importance of system updates.	Updates, or patches, fix known vulnerabilities, preventing adversaries from using documented exploits.	
	4.3.D: Configure a host-based firewall.	Host-based firewalls protect single devices using Access Control Lists (ACLs) that apply the first matching rule in sequence to permit or deny inbound and outbound traffic based on IP, port, or service.	
DAY 13-16 4.4 Detecting Attacks on Devices	**4.4.A:** Explain how to detect attacks.	Indicators of Compromise (IoCs) can be host-based (unexpected processes/unauthorized settings), file-based (malicious file hashes/paths), or behavior-based (failed logins/unusual times or locations).	**Scenario 4C: Dynamic Forensic Analyst logs**; EDR (Endpoint Detection and Response) service descriptions; AI for anomaly detection. **Scenario 4C:** Students analyze authentication logs for signs of password spraying or credential stuffing on a manufacturing network and submit a forensic report of findings.
	4.4.B: Determine detection controls.	Criteria for detection methods include performance (anomaly-based tools use more memory/CPU), cost (software licensing or EDR services), and the sensitivity of the device.	
	4.4.C: Evaluate the impact of detection.	Factors include detection speed, impact on device performance, and the trade-off between false positives (low in signature-based tools) and the ease of bypass for adversaries.	
	4.4.D: Apply detection techniques to log files.	Techniques include identifying password spraying (many users failing within seconds from one IP) or credential stuffing (repeated attempts of default user:password combos). Note that offline attacks cannot be detected because they occur on the adversary's computer.	

Unit Title:

Unit 5: Securing Applications and Data

Relevant Standards: Bold indicates priority

Skill 2: Mitigate Risk - Implement protective and deterrent security controls.

2.A Identify security controls, and explain how they mitigate risks.
2.B Determine layered security controls that address vulnerabilities.
2.D Implement and log mitigations with and without the support of AI.

Skill 3: Detect Attacks - Implement detection methods, monitor systems, and analyze evidence.

3.B Determine strategies and methods to detect attacks.
3.D Detect and classify cyberattacks by analyzing digital evidence with and without the support of AI.

Skill 4: Collaborate - Work with others and AI to accomplish a task.

4.A Develop clear, shared team objectives related to a cybersecurity task.
4.B Determine clear roles and responsibilities for members of a team working to accomplish a cybersecurity task.
4.C Implement AI as a collaboration tool individually and as a group.
4.D Complete assigned work to accomplish a collaborative cybersecurity task.

Essential Question(s):

- How does an adversary's ultimate goal of stealing, modifying, or denying access to data influence their choice of application-level attack methods, such as SQL injection, Cross-Site Scripting (XSS), or buffer overflows?
- How do the various states of data dictate the degree of security controls and cryptographic methods required to protect its confidentiality and integrity?
- In what ways do legal and regulatory frameworks, such as HIPAA for health information and PCI-DSS for payment information, mandate specific data classification and handling practices for organizations?
- How do different access control models implement the principle of least privilege to restrict unauthorized operations on sensitive files?
- What are the fundamental differences between symmetric and asymmetric cryptography, and how does the secure management of private keys impact the security of an entire encrypted system?
- Why are the principles of "secure by design" and "security by default" critical for software developers, and how does user input sanitization serve as a primary defense against directory traversal and injection attacks?
- How can security analysts differentiate between normal user behavior and indicators of compromise (IoCs) in accounting and web server logs to detect active application-layer attacks?
- What are the operational impacts and technical trade-offs of using automated detection tools like honeypots and Data Loss Prevention (DLP) compared to retrospective log analysis and hash verification?

Enduring Understanding(s):

- Data is the core of the digital world, and stealing, modifying, or denying access to data is the primary end goal for most adversaries.
- The value and sensitivity of data are not uniform; the perceived value and regulatory classifications (such as PII, PHI, or PCI) directly influence the risk assessment and the degree of security controls required.
- Effective security requires distinct strategies for data in different states: at rest (stored), in transit (moving), and in use (processing).
- Organizations must enforce strict access control models to uphold the principle of least privilege, ensuring users have only the minimum access necessary for their roles.
- Cryptography is the primary tool for maintaining confidentiality; symmetric encryption uses a single shared key, while asymmetric encryption uses public and private key pairs to allow secure communication without prearranged secrets.
- Cryptographic hash functions are vital for ensuring data integrity; because hashes are repeatable and sensitive to even minor changes, they allow defenders to detect if a file has been altered by an adversary.
- Securing applications requires moving beyond "add-on" features toward "secure by design" and "security by default" principles, with user input sanitization serving as a critical defense against injection and traversal attacks.
- Defenders must utilize a combination of real-time tools and retrospective accounting log analysis to identify indicators of compromise (IoCs) and unauthorized access patterns.

Demonstration of Learning:

Authentic unit scenarios designed to connect cybersecurity concepts to real-world personal security situations (see Lesson Sequence).

Formal demonstration of learning is measured through the AP Exam

Pacing for Unit

19 Block Periods

- Topic 5.1: Application and Data Vulnerabilities and Attacks: ~ 3 Blocks
- Topic 5.2: Protecting Applications and Data: Managerial Controls and Access Controls: ~ 4 Blocks

• Multiple Choice: Weighs Skill Category 1 (Analyze Risk), Skill Category 2 (Mitigate Risk), and Skill Category 3 (Detect Attacks) equally at 25–40% each across the entire course content. • Free-Response Question (FRQ): Security Analysis FRQ directly assesses Unit 5 skills. Students must analyze simulated sources, such as file-system permissions and application log files, to identify security issues and write the correct commands to remediate vulnerabilities.	• Topic 5.3: Protecting Stored Data with Cryptography: ~ 3 Blocks • Topic 5.4: Asymmetric Cryptography: ~ 3 Blocks • Topic 5.5: Protecting Applications: ~ 2 Blocks • Topic 5.6: Detecting Attacks on Data and Applications: ~ 4 Blocks
Family Overview (link below)	**Integration of Technology:**
AP Cybersecurity Family Overview	• Encryption Suites • Secure Messaging • Hashing Utilities • Linux Permissions • Role-Based (RBAC) models • Discretionary (DAC) models • Mandatory (MAC) models • Artificial Intelligence (AI) as a Technical Partner • Nginx web server logs and accounting logs • Deployment of honeypots and Data Loss Prevention (DLP) services • Intrusion Prevention Systems (IPS)
Unit-specific Vocabulary:	**Aligned Unit Materials, Resources, and Technology (beyond core resources):**
• Data at Rest • Data in Transit • Data in Use: • PII (Personally Identifiable Information). • PHI (Protected Health Information) • PCI (Payment Card Information) • Subject • Object • Role-Based Access Control (RBAC) • Rule-Based Access Control (RuBAC) • Discretionary Access Control (DAC) • Mandatory Access Control (MAC) • Principle of Least Privilege • Data Validation • Input Sanitization • SQL Injection • Cross-Site Scripting (XSS) • Buffer Overflow • Directory Traversal: • Plaintext • Ciphertext • Symmetric Encryption • Asymmetric Encryption • Keyspace • Block Encryption • Stream Encryption • Accounting • Honeypot • DLP (Data Loss Prevention • Retrospective Analysis	N/A
Opportunities for Interdisciplinary Connections:	**Anticipated misconceptions:**

• Privacy Law: Students study the Privacy Act of 1974 and the Children's Online Privacy Protection Act (COPPA) in the context of protecting Personally Identifiable Information (PII). • Healthcare Regulation: The unit introduces HIPAA (1996), which mandates strict security for Protected Health Information (PHI) • Financial Standards: Students learn about the Payment Card Industry Data Security Standard (PCI DSS), which regulates how organizations must store and transmit credit card data. • Proprietary Research: Students act as security team members for a pharmaceutical company tasked with protecting research on a new product, connecting cybersecurity to the biotech R&D process and the importance of intellectual property. • Bioethics: The classification of health records as highly sensitive (PHI) connects to broader ethical discussions about patient privacy and medical confidentiality. • Algorithmic Functions: Students explore the mechanics of symmetric and asymmetric encryption, which rely on mathematical algorithms to hide information in ciphertext • Mathematical Inverses: The study of asymmetric cryptography involves learning about public and private key pairs, which are mathematical inverses where one key reverses the operation of the other. • Organizational Policy: Students analyze and identify the components of Cryptography Policies and Web Application Security Policies, mirroring the work of business compliance officers • Operational Risk: The curriculum connects data classification (at rest, in transit, in use) to business priorities, teaching students to prioritize security controls based on the criticality and value of the data to an organization • Critical Infrastructure: Students simulate security engineers at a utility company that owns power generating plants, exploring the necessity of secure communication for maintaining the stability of national energy systems.	• Public vs. Private Key Usage • Misinterpreting Linux Permission Bits • Entity Confusion • The "+" Symbol • Hashing vs. Encryption Purposes • "Secure by Design" as a Post-Development Feature • The Scope of Input Sanitization • Directory Traversal as "Normal" Navigation • Data State Protection Fallacies • The "Authenticity" of Honeypots
Connections to Prior Units:	**Connections to Future Units:**
• Integration into the Defense-in-Depth Model: Unit 5 represents the innermost layer of the defense-in-depth (layered defense) strategy introduced in Unit 2. While prior units focused on the physical perimeter (Unit 2), the network (Unit 3), and the device (Unit 4), Unit 5 addresses the ultimate objective of most adversaries: the applications and data itself. Students learn that if all other layers are bypassed, these final controls are the last line of defense. • Application of the Risk Assessment Framework: The formal risk assessment process defined in Unit 2 is applied directly to data in Unit 5. Students move from assessing physical or network risks to evaluating the risk to specific data classifications, such as: ○ PII (Personally Identifiable Information): Covered by laws like the Privacy Act.	N/A

- PHI (Protected Health Information): Regulated by HIPAA.
- PCI (Payment Card Information): Regulated by industry standards.

- Evolution of Cryptographic Concepts: Unit 5 builds upon the cryptographic foundations laid in Unit 4:
  - From Hashing to Encryption: In Unit 4, students mastered cryptographic hashing for password storage and integrity. Unit 5 expands this into two-way encryption for maintaining confidentiality, teaching both symmetric (AES) and asymmetric (RSA/ECC) algorithms.
  - Integrity Verification: The hashing skills from Unit 4 are used in Unit 5 as a detective control to verify if files have been altered by an adversary.
- Scaling Access Control and Authorization: Unit 5 evolves the basic login settings from Unit 1 and the local device hardening from Unit 4 into formal Access Control Models:
  - Models: Students apply the principles of least privilege using Role-Based (RBAC), Discretionary (DAC), and Mandatory Access Control (MAC) models.
  - Technical Skills: The Linux-style file permission skills (rwx) introduced in Unit 4 assessments are moved into active configuration in Unit 5 Scenario 5A, where students must use the chmod command to protect proprietary research.
- Maturation of Log Analysis and Detection: The practice of identifying Indicators of Compromise (IoCs) becomes its most sophisticated in Unit 5:
  - Progression: Students move from simple unauthorized logins (Unit 1) and network-based traffic patterns (Unit 3) to application-layer forensics.
  - Specific IoCs: Unit 5 requires students to find evidence of advanced attacks in web server logs, such as SQL injection control words (e.g., OR 1=1), XSS script tags, and directory traversal sequences (../).
- Protection Across Data States: Unit 5 expands on the concept of data in transit (the focus of Unit 3 network security) by introducing protection strategies for data at rest (stored on drives) and data in use (actively being processed). Students learn that data must be unencrypted to be used, necessitating the strict access controls studied earlier in the unit.
- Continuous Use of AI as a Collaboration Tool: Building on Skill 4.C introduced at the start of the course, Unit 5 continues to integrate Artificial Intelligence as a technical partner. Students use AI to help analyze application code for vulnerabilities and to summarize complex digital events in web server logs that are too vast for human review.

Differentiation through *Universal Design for Learning*

	Engagement	Representation	Action & Expression
5.1A	OWASP Top 10 interactive lab exploring software application exploits.	Flowcharts mapping software flaws (buffer overflows, injection) to system impact.	Create an application security awareness flyer or record a video briefing.
5.1B	Hands-on lab using WebGoat/Juice Shop executing SQL Injection (SQLi) and XSS.	Side-by-side code visual showing dynamic query building vs. parameterized queries.	Write a code vulnerability walkthrough or present an exploit analysis video.
5.1C	Threat-modeling exercise applying STRIDE to web application architectures.	STRIDE threat model template paired with a severity rating matrix.	Submit a completed STRIDE Threat Model report for a target web application.

5.2A	Sorting activity categorizing data states (Rest, Transit, Use) and sensitivity levels.	Grid mapping data classifications to appropriate security controls (TLS, AES).	Draft a Data Classification Standard document or design an organizational guide poster.
5.2B	Case study evaluation of Data Loss Prevention (DLP) and compliance frameworks.	Policy framework chart illustrating data retention, privacy, and DLP governance.	Write a corporate Data Privacy Policy memo or construct a compliance slide deck.
5.2C	Role-play exercise contrasting DAC, MAC, RBAC, and ABAC in enterprise scenarios.	Comparison matrix evaluating DAC, MAC, RBAC, and ABAC access models.	Design an Access Control Matrix for a healthcare or financial system model.
5.2D	Linux CLI lab configuring user file permissions (chmod, chown, POSIX ACLs).	Visual octal permissions diagram mapping rwx / 755 / 644 values.	Submit a bash script configuring Linux permissions or record a video walkthrough.
5.3A	Local file encryption lab using BitLocker or VeraCrypt to test unauthorized access.	Flowchart showing plaintext converted to ciphertext via encryption keys.	Draft an "Encryption at Rest" user guide or demonstrate file encryption in a video.
5.3B	Command-line lab using OpenSSL to encrypt/decrypt text files using AES-256.	Visual diagram illustrating shared secret key usage for encryption and decryption.	Submit an OpenSSL execution portfolio or write a technical secret key guide.
5.4A	"Public Key Exchange" activity sending encrypted notes between peers using GPG.	Key pair diagram (Public Key = Lock, Private Key = Key) illustrating workflows.	Construct a Public Key Infrastructure (PKI) flowchart or create a video lesson.
5.4B	Key space math challenge calculating brute-force times across 56-bit to 256-bit keys.	Exponential graph illustrating key bit length vs. computational brute-force entropy.	Write an analytical paper on cryptographic key strength or deliver a presentation.
5.4C	Hands-on CLI lab generating GPG key pairs, exchanging public keys, and decrypting messages.	Step-by-step workflow graphic showing GPG key generation and message signing.	Submit an encrypted and signed message portfolio or record a GPG screencast.
5.5A	Software critique activity evaluating weak default settings in commercial applications.	Principles graphic illustrating least privilege, fail-safe defaults, and defense in depth.	Draft a Secure Coding Standard document or deliver a presentation to mock developers.
5.5B	Web form lab submitting script payloads (<script>alert(1)</script>) to test sanitization.	Input pipeline diagram showing raw input -> sanitization/encoding -> execution.	Write code snippets demonstrating input validation or record an instructional video.
5.6A	Lab inspecting File Integrity Monitoring (FIM) tools and database activity logs.	Architecture diagram showing Database Activity Monitoring (DAM) and FIM alerts.	Create a data breach detection guide or write a data exfiltration forensic report.
5.6B	Selection scenario matching Web Application Firewalls (WAF) and DB auditing tools.	Matrix mapping attack types (SQLi, XSS, file tampering) to detection controls.	Propose an application detection strategy for a web application deployment.
5.6C	Analyze performance latency and false positive rates when running WAF in blocking mode.	Trade-off chart balancing web performance impact against threat detection coverage.	Deliver an impact evaluation presentation or write an executive technical review.
5.6D	"Tamper Detection Challenge" calculating MD5/SHA-256 hashes of modified files using sha256sum.	Side-by-side visual showing how a single character change alters the hash output.	Submit a file verification lab report or record a video tutorial on hashing.
5.6E	Web server log analysis lab searching access logs for SQLi payloads and directory traversal.	Color-coded HTTP log cheat sheet mapping status codes (200, 403, 500) and signatures.	Write an application incident report based on web log analysis or give a presentation.

Supporting Multilingual/English Learners (*CELP standards*)

	Emerging	Expanding	Bridging
5.1A	Match application attack types (e.g., *SQL injection, Buffer overflow, Cross-Site Scripting/XSS*) to visual code/web diagrams.	Explain how input vulnerabilities lead to unauthorized application control using cause-and-effect sentence frames.	Analyze application vulnerability mechanisms and trace how malicious payloads exploit memory or database logic.
5.1B	Trace data flow in a visual diagram showing malicious input bypassing input fields directly into a database.	Describe application exploitation steps using sequential transition words and technical vocabulary.	Detail exploit mechanisms across OWASP Top 10 web application vulnerabilities.

5.1C	Complete an application risk assessment worksheet using color-coded severity cards.	Write application risk summaries using a standardized template (*Vulnerability, Threat, Impact, Risk Score*).	Perform threat modeling (e.g., STRIDE framework) for web applications and document systemic data risks.
5.2A	Sort data items (e.g., *Public website text, Student SSNs, Medical records*) into classification buckets (*Public, Internal, Confidential, Restricted*).	Explain how data classification levels dictate security controls (encryption, access limits) using comparative structures.	Formulate an enterprise data classification matrix and map corresponding data lifecycle security requirements.
5.2B	Match managerial controls (e.g., *NDAs, Data Retention Policies, Separation of Duties*) to definition cards.	Describe administrative policies protecting sensitive application data using formal regulatory language.	Author data governance and privacy policy frameworks compliant with legal standards (e.g., FERPA, GDPR, Privacy Act).
5.2C	Match scenario cards to Access Control Models (*DAC, MAC, RBAC, ABAC*) using visual feature descriptions.	Recommend access control models (e.g., *Role-Based vs. Attribute-Based*) for organization scenarios using decision templates.	Evaluate organizational access requirements and design scalable Role-Based (RBAC) and Attribute-Based (ABAC) structures.
5.2D	Execute guided Linux file permission commands (chmod, chown) following a visual syntax guide card (rwx permissions table).	Configure Linux file permissions and ownership via command line, documenting permission numeric codes (chmod 750).	Manage complex POSIX file permissions and Access Control Lists (setfacl) on Linux systems to enforce least privilege.
5.3A	Match encryption concepts (e.g., *Plaintext + Key $\rightarrow$ Ciphertext*) to visual block diagrams.	Explain confidentiality protection via encryption using guided paragraphs ("*Encryption converts unreadable ciphertext so that...*").	Evaluate cryptographic security states (*Data at Rest, Data in Transit, Data in Use*) and corresponding protective schemes.
5.3B	Encrypt and decrypt short messages using a simple visual cipher wheel or tool (e.g., CyberChef Caesar/AES demo) with step-by-step guidance.	Demonstrate symmetric encryption concepts using shared secret keys and explain key distribution limitations using sentence starters.	Implement symmetric encryption algorithms (AES) in CLI/lab tools and analyze key management challenges.
5.4A	Use a key-pair visual diagram prompt card: "*To encrypt for Alice, use Alice's [Public Key]. To sign, Alice uses her [Private Key]*".	Explain key usage rules in asymmetric cryptography using conditional sentence frames ("*When sending a secret message to Bob, Alice uses...*").	Solve complex Public Key Infrastructure (PKI) scenario problems involving digital signatures, encryption, and non-repudiation.
5.4B	Compare key length visual charts showing time required to brute-force 56-bit vs. 128-bit vs. 256-bit keys.	Explain the relationship between key length, exponential combinations (2^n), and brute-force difficulty using structured prompts.	Quantify cryptographic strength computationally and explain how key length protects against modern brute-force systems.
5.4C	Encrypt/decrypt short messages using an interactive PKI demonstration web application with visual step-by-step prompts.	Execute asymmetric encryption/decryption tasks using tools (e.g., GPG) and document public/private key exchanges.	Generate PGP/GPG keypairs, manage key rings, and perform signed and encrypted file exchanges in CLI environments.
5.5A	Match security principles (*Secure by Design, Security by Default*) to visual example cards (e.g., *all ports closed by default*).	Explain *Secure by Design* and *Security by Default* principles using comparative graphic organizers.	Audit application deployment configurations against *Secure by Design* principles and recommend hardening strategies.
5.5B	Complete a visual contrast card showing raw input with malicious code vs. sanitized/escaped code input.	Explain how input sanitization prevents injection attacks using sentence frames ("*Sanitization neutralizes code by stripping...*").	Evaluate input validation, parameterization, and output encoding techniques across software development scenarios.
5.6A	Circle abnormal data access behaviors (e.g., *mass file downloads at 3 AM*) on a visual security dashboard mockup.	Describe indicators of data exfiltration and unauthorized access using targeted technical language.	Analyze data loss prevention (DLP) metrics and database audit logs to identify complex data breach attempts.
5.6B	Match application detection controls (e.g., *WAF, Database Activity Monitoring, DLP*) to threat scenario cards.	Select and justify application layer detection controls using decision matrix templates.	Design comprehensive application monitoring architectures integrating Web Application Firewalls (WAF) and SIEM logging.
5.6C	Sort impacts of detection methods into a visual chart (*System Latency, Blocked Legitimate Users, Caught Attacks*).	Evaluate trade-offs between strict application monitoring rules and system performance/usability using guided templates.	Conduct impact evaluations of WAF rule configurations balancing security efficacy against false-positive rates.

5.6D	Compare two MD5/SHA-256 hash strings side-by-side and indicate if they match or differ (*Same = Unaltered, Different = Altered*).	Verify file integrity by computing hash digests via command line (sha256sum) and writing verification statements.	Automate file integrity monitoring (FIM) scripts to detect unauthorized file modifications across system directories.
5.6E	Highlight web server log lines showing common attack patterns (e.g., ' OR '1'='1, <script>) in pre-formatted log sheets.	Analyze HTTP access logs (e.g., Apache/Nginx logs) to identify attack signatures and write incident summary reports.	Parse, filter, and analyze web application access and error logs to trace multi-stage web application compromises.

Unit Outline

Lesson Sequence	Learning Target	Success Criteria	Assessment
DAY 1-3 5.1 Application & Data Risks	**5.1.A:** Explain how adversaries can exploit application and file vulnerabilities to cause loss, damage, disruption, or destruction.	Adversaries can read unencrypted files if they have device access, exploit elevated administrative privileges on compromised accounts, or take advantage of weak access control settings to steal or destroy files.	Examples of SQLi, XSS, and directory traversal; AI-powered tools for risk evaluation. Students can identify injection-type attacks (SQLi, XSS) and buffer overflows. They produce a risk assessment for sensitive data, such as unencrypted jet engine specs, documenting likelihood and impact.
	5.1.B: Explain how application attacks exploit vulnerabilities.	Vulnerabilities include a lack of data validation and input sanitization. Specific attacks include SQL injection (inserting database commands), Cross-Site Scripting (XSS) (injecting malicious browser code), buffer overflows (overwriting memory), and directory traversal (using ../ sequences to access unauthorized system files)	
	5.1.C: Assess and document risks from application and data vulnerabilities.	Risks involve compromises to confidentiality, integrity, and availability. High risks involve highly sensitive or regulated data such as PHI or PII stored on unencrypted drives, while low risks involve less sensitive info with shorter encryption keys	
DAY 4-7 5.2 Access Controls	**5.2.A:** Explain how the state or classification of data impacts the type and degree of security applied to that data.	Security depends on whether data is at rest (stored), in transit (moving), or in use (processing) Laws like HIPAA (PHI) and PCI-DSS (payment info) mandate specific storage and handling rules for regulated data	**Scenario 5A: Protecting Sensitive Data**; RBAC, RuBAC, DAC, MAC; Linux terminal or BASH emulator. **Scenario 5A:** Students apply the principle of least privilege to secure a pharmaceutical lab's air-gapped computer. They successfully use the Linux chmod command to set specific read, write, and execute permissions for directories.
	5.2.B: Identify managerial controls related to application and data security.	Managerial controls include Cryptography Policies (defining approved algorithms and key lengths) and Web Application Security Policies (setting timelines for vulnerability remediation)	
	5.2.C: Determine an appropriate access control model to protect applications and data.	Models include Role-Based (RBAC), Rule-Based (RuBAC), Discretionary (DAC), and Mandatory Access Control (MAC) The Bell-LaPadula model (MAC) uses "write up, read down" to protect information	

	5.2.D: Configure access control settings on a Linux-based system.	Students must use the chmod command to set read, write, and execute (rwx) permissions for the owner, group, and others using both numeric and symbolic methods	
DAY 8-10 5.3 Symmetric Cryptography	**5.3.A:** Explain how encryption can be used to protect files.	Cryptography hides plaintext to produce ciphertext. Algorithms are classified as symmetric (one key) or asymmetric (two keys) and may use block or stream encryption methods	**Symmetric Encryption:** OpenSSL tool; Cryptography policies. Students understand the CIA triad of data at rest, in transit, and in use. They use the OpenSSL CLI to encrypt a test file with a 128-bit AES key and then decrypt it using the correct password.
	5.3.B: Apply symmetric encryption algorithms to encrypt and decrypt data.	Advanced Encryption Standard (AES) is the most common symmetric algorithm. Students use tools like OpenSSL to perform encryption and decryption tasks	
DAY 11-13 5.4 Asymmetric Cryptography	**5.4.A:** Determine the appropriate asymmetric key to use when sending or receiving encrypted data.	Asymmetric encryption uses a public key (to encrypt) and a private key (to decrypt) The keys are mathematical inverses, and the security of the system depends on keeping the private key secret	**Scenario 5B: Sending Encrypted Messages**; **Asymmetric Encryption)**; PGP or RSA encryption tools. **Scenario 5B:** Students generate an RSA key pair, share their public key with a partner, and successfully send/receive an encrypted secret message while maintaining private key security.
	5.4.B: Explain why the length of a key impacts the security of encrypted data.	Longer keys increase the keyspace, making it harder for software to guess keys as computational power improves	
	5.4.C Apply asymmetric encryption algorithms to encrypt and decrypt data.	Common algorithms include RSA and Elliptic Curve Cryptography (ECC). Students demonstrate the use of CLI commands to generate key pairs and encrypt/decrypt files	
DAY 14-15 5.5 Secure by Design	**5.5.A:** Identify the application security principles of secure by design and security by default.	Secure by design makes security a core principle in all development phases. Security by default ensures security features are enabled out of the box.	Web application security policies; Input sanitization function examples. Students can evaluate code to ensure companies take ownership of security outcomes. They explain how removing control characters (like ' or --) prevents SQLi and XSS.
	5.5.B: Explain how user input sanitization protects applications.	Programmers must use verification functions to remove malicious characters (like single quotes or semicolons) to prevent SQL injection, XSS, and directory traversal.	
DAY 16-19 5.6 Detecting Data Attacks	**5.6.A:** Explain how to detect attacks on data.	Analysis of accounting logs can reveal unusual file access patterns. Defenders can use honeypots (fake files containing fake PII) or cryptographic hashes to detect if data has been unexpectedly altered	**Honeypots and DLP services**; Windows PowerShell or BASH for hashing; Log entries from Source 4. Students analyze web application and server logs to identify indicators of compromise (IoCs), such as <script> tags for XSS or OR 1=1 for SQLi. They verify file integrity by comparing SHA256 hashes.
	5.6.B: Determine controls for detecting attacks against applications or data.	Criteria include cost, the criticality of the data, and regulatory data classification requirements	
	5.6.C: Evaluate the impact of a method for detecting attacks against an application or data.	Automation is required for effective log analysis. Tools like Data Loss Prevention (DLP) and honeypots provide real-time alerts but may produce false negatives if an adversary steals data without altering it.	

	5.6.D: Identify whether a file has been altered by verifying its hash.	Students use CLI commands like Get-FileHash (PowerShell) or sha256sum (BASH) to compare hash outputs over time; a changed hash indicates the file was altered	
	5.6.E: Apply detection techniques to identify and report indicators of application attacks by analyzing log files.	Detection signatures include SQL control words (WHERE, OR 1=1), HTML script tags for XSS, long URL strings for buffer overflows, and ../ sequences for directory traversal	